Quadro2x

The Global Phone Network in a Box

Manual II:
Administrator's Guide
for Quadro2x and Quadro2xi

Edition 1, SW Release 3.1.7 and higher, January 2006

Table of Contents

Manual III: see Extension User's Guide
Describes detailed the menus available for extension users and includes all call codes at a glance.

About this Administrator's Guide

The Quadro Manual is divided into three parts:

- **Manual I: Installation Guide**
  gives step-by-step instructions to provision the Quadro and configure the phone extensions with the Epygi SIP Server. After successfully configuring the Quadro, a user will be able to make SIP phone calls to remote Quadro devices, make local calls to the PSTN and access the Internet from devices connected to the LAN.
- **Manual II: Administrator's Guide** explains all Quadro management menus available for administrators only and includes a list of all System Default Values.
- **Manual III: Extension User's Guide** explains all Quadro management menus available for extension users. A list of all call codes can be found there, too.

This Administrator's Guide explains all Quadro2x models: Quadro2x and Quadro2xi.

This manual contains many example screen illustrations. Since Quadro devices offer a wide variety of features and functionality, he example screens shown may not appear exactly the same for your particular Quadro as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

Quadro's Graphical Interface describes the Quadro's graphical user interface and explains all recurrent buttons.

Administrator's Menus explains the Administrator's management pages according to the menu structure shown on the main page of the Quadro management.

Administrator's Additional Features explains some input-options for administrators only that may be selected from the extension user's main page.

Appendix: Extension Users Welcome Page includes a preprinted MS-Word form that allows the administrator to inform his extension user of all individually needed addresses and phone numbers.

Appendix: System Default Values lists all factory defaults.

Appendix: Software License Agreement includes the contract for using Quadro's hardware and software.

Quadro's Graphical Interface

Administrator's Main Page

As the result of logging in as an administrator, the page **Quadro Management** is displayed with a table of active calls (including information about call peers, call duration and start time) at the startup. Here the administrator may access the following settings and perform the actions:

Fig. II-1: Quadro2x Management

System Menu
- System Configuration Wizard
- Internet Configuration Wizard
- Status
- IP Routing Configuration
- Configuration Management
- Events
- Time/Date Settings
- Mail Settings
- SMS Settings
- Firmware Update
- Networking Tools
- Diagnostics
- Automatic Provisioning
- Features
- Upload Language Pack
- User Rights Management

Telephony Menu
- Call Statistics
- SIP Settings
- RTP Settings
- NAT Traversal Settings
- Line Settings
- FXO Settings
- ISDN Settings
- Gain Control
- Call Routing
- VoIP Carrier Wizard
- RADIUS Client Settings
- Voice Mail Common Settings
- Dial Plan Settings

Internet Uplink Menu
- PPP/ PPTP Settings
- VPN Configuration
- Dynamic DNS Settings
- Firewall and NAT
- Filtering Rules
-

Users Menu
- Extensions Management
- Receptionist Management

LAN Services Menu
- DNS Settings
- DHCP Settings for the LAN Interface

Registration Form
(in menu tree only)

Logout

The functional button **Renew Wan IP Address** appears on the administrator's main **Quadro Management** page if the Quadro device acts as a DHCP client. The **Renew WAN IP Address** button is used to get a new WAN IP address in case, e.g., the Quadro moves to another network.
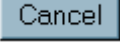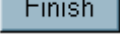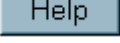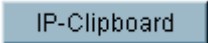
The functional button **Establish Your Internet Connection Now** respectively **Terminate Your Internet Connection Now** occurs on the Quadro Management page if PPPoE is used as WAN interface protocol.

The link **Please Check Your Pending Events** will be displayed on the administrator **Main Menu** page if new system events exist. The link leads to the **Events** page that can be also accessed from the System menu.

The list of **Users currently logged into the system** is seen in the lower right corner of the Administrator's Main Menu. Information about IP address user accessed Quadro GUI from, the username user is logged in and the time until the next automatically logout is provided herein. The idle session timeout is set to 20 minutes. If no action is performed during that time, user will be automatically moved to the Login page and will be requested to login again.

The link **Refresh in** occurs in the upper right corner beside the field displaying the number of seconds until the next refresh and is used to perform a manual reload of the page. If a page with a Refresh counter is left opened, the session time-out counter will be updated periodically and the logout timeout will never expire.

Recurrent Buttons

Button	Description	Button	Description
Previous	This button leads back to the previous page of a fixed sequence of pages (used mainly in wizards).	Back	This button leads back to the page you have been on before.
Next	This button leads onward to the next page of a fixed sequence of pages (used mainly in wizards).	Ok	This button confirms an operation you started before.
Cancel	This button discards the latest, not yet confirmed entries.	Yes	This button confirms an operation you chose before.
Finish	This is the last button of a fixed sequence of pages that completes and saves the entries of the whole sequence.	No	This button discards an operation you chose before.
Help	This button opens the help page belonging to the currently active Quadro management page.	Save	This button saves the settings modified on the currently active management page.
IP-Clipboard	This button opens a window where the last inserted IP addresses are listed. It is a kind of clipboard that helps the user to make quick selection of an IP address in case it has been already used in the past, thus to avoid typing it again. The clipboard can hold up to 10 IP addresses, a new IP address will replace the oldest one from the list.	SIP Clipboard	This button opens a window where the last inserted SIP addresses are listed. It is a kind of clipboard that helps the user to make quick selection of a SIP address in case it has been already used in the past, thus to avoid typing it again. The clipboard can hold up to 10 SIP addresses, a new SIP address will replace the oldest one from the list.

Recurrent Functional Buttons

In connection with tables, the following buttons - among others - usually occur:

Functional Button	Description
Add	Allows adding a new record to the displayed table. A new page will be displayed to enter any new settings.
Edit	Allows modifying the settings of the record selected by its checkbox. Normally only one record may be selected. A new page will be displayed to enter the modified settings.
Delete	Deletes the selected entry(s) of a table. A warning message will demand a confirmation before deleting an existing entry.
Select All	Selects all table entry(s)for example for further deletion.
Inverse Selection	Inverses an existing selection of table entry(s). If no entries are selected, clicking the button will select all records.
Refresh in...	May occur in the upper right corner of a page. It displays the number of seconds remaining until the next refresh of the page and it may be used to reload the page manually.

Most of the tables offer the option to sort the entries in ascending or descending order by clicking the headings of the columns. A small arrow beside the column heading will show the direction of sorting - upward or downward. The entries of the table can be selected by the assigned checkboxes - one at a time, for the most part - in order to edit or delete them.

Entering a SIP Addresses correctly

Calls over IP are implemented based on Session Initiating Protocol (SIP) on the Quadro. When making a call to a destination that is somewhere on the Internet, SIP address must be given.

SIP addresses have to be specified in one of the following formats:

"display name" <username@ipaddress:port>
"display name" <username@ipaddress>
username@ipaddress:port
username@ipaddress
username

Particularly the following combinations can be used for your convenience:

- *@ipaddress - any user from the specified SIP server
- username@* - a specified user from any SIP server
- *@* - any user from any SIP server

The display name and the port number are optional parameters in the SIP address. If a port is not specified, 5060 will be set up as the default one. The range of valid ports is between 1024 and 65536.

A flexible structure of wildcards is allowed. In comparison with a wildcard, the "?" character stands for only one unknown digit and the "*" character stands for any number of any digits.

Please Note: Wildcards are available for caller addresses only. No wildcard characters are allowed for called party addresses. Exceptions are addresses in **Supplementary Addresses** table which are used by **Outgoing Call Blocking** and **Hiding Caller Information Settings** services. To use "*" and "?" themselves (as non wildcard characters), use "*" and "\?" correspondingly.

Administrator's Menus

System Menu

Fig. II-1: System Menu in Dynamo theme

Fig. II-2: System Menu in Plain theme

System Configuration Wizard

The **System Configuration Wizard** is the helpful tool for the administrator to define the Quadro's Local Area Network settings and to specify regional configuration settings to make Quadro operational in its LAN. The **System Configuration Wizard MUST be run upon Quadro's first startup** to make sure that it works properly in its network environment. The Wizard allows navigating through the following basic configuration parameters and settings:

- System Configuration (see below)
- DHCP Settings for the LAN Interface
- Regional Settings and Preferences (see below)
- Emergency Codes and PSTN Access Codes Settings (see below)

DHCP Settings for LAN are described in the chapters below while LAN configuration and regional settings will be described in the current chapter.

Please Note: It is strongly recommended to leave the factory default settings if their meanings are not fully clear to the administrating person.

Fig. II-3: System Configuration Wizard - Start page

The **System Configuration** page contains the host name, IP address and Subnet Mask information about the Quadro LAN interface. These settings make Quadro available to the internal network.

The **System Configuration** page offers the following input options:

Host Name requires a host name for the Quadro device.

IP Address requires the Quadro host address for the LAN interface.

Subnet Mask requires the Quadro hosts' Subnet Mask.

Fig. II-4: System Configuration Wizard - System Configuration page

The **Regional Settings and Preferences** are used to select settings specific to the location of the Quadro.

This is important for the functionality of the voice subsystem.

The **Regional Settings and Preferences** page has two drop down lists to select the **Location** (country) and a corresponding **Timezone** and a manipulation radio button group to choose:

- **System Language** – selection is available only when custom Language Pack has been uploaded and is used to enable custom language for system voice messages or turn back to default (English).

- **GUI Theme** - selection used to select the GUI theme style of the web based configuration pages.

Fig. II-5: System Configuration Wizard - Regional Settings page

The **Emergency Codes** and **PSTN Access Codes Settings** are used to configure the dial plan parameters used in the routing mode.

The **Emergency Codes** text field requires the PSTN numbers of the emergency or lifeline services. Multiple emergency codes, separated by commas, can be inserted in this field. For each emergency code, a routing pattern will be generated in the Call Routing Table, which will allow to make fast and easy calls to emergency destinations.

The **PSTN Access Code** drop down list allows to select the prefix code for accessing the PSTN line in the routing mode. Dialing the digits inserted in this text field will provide the PSTN dial tone, when acting in the routing mode or making routing calls (for routing calls an additional "0" will need to be dialed first.)

Fig. II-6: System Configuration Wizard - Emergency Codes and PSTN Codes Settings page

Internet Configuration Wizard

The **Internet Configuration Wizard** is the helpful tool for the administrator to configure the WAN interface settings and to adjust Quadro's connectivity with an external network. The **Internet Configuration Wizard MUST be run if it is desired for Quadro to be connected to the Internet**.

All the settings of the **Internet Configuration Wizard** are described in the chapters below except those for the IP settings, which will be described in this chapter.

Please Note: It is strongly recommended to leave the factory default settings if their meanings are not fully clear to the administrating person.
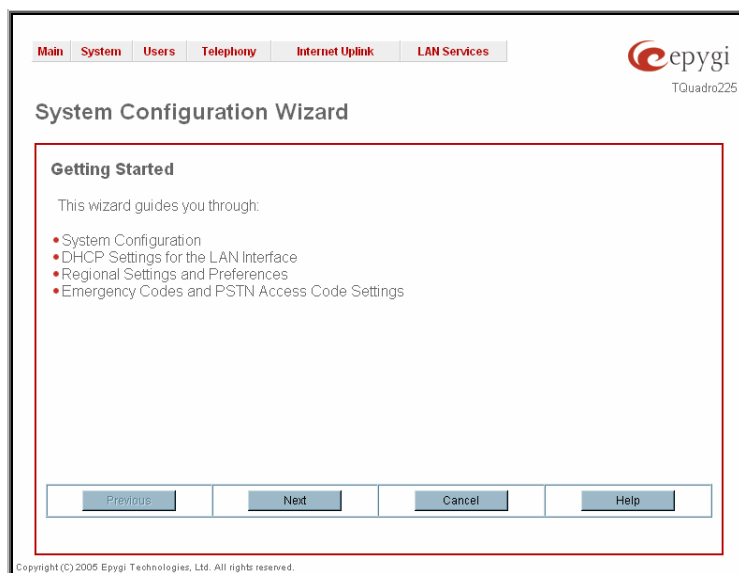
Fig. II-7: Internet Configuration Wizard - Start page

The Wizard allows navigating through the following basic configuration parameters and settings:

- Uplink configuration (see below)

For WAN Interface protocol **PPPoE**:

- PPP/ PPTP Settings
- WAN Interface Configuration (see below)
- DNS Settings

For WAN Interface protocol **PPTP**:

- WAN IP Configuration (see below)
- PPP/ PPTP Settings
- WAN Interface Configuration (see below)
- DNS Settings

For WAN Interface protocol **Ethernet**:

- WAN IP Configuration
- WAN Interface Configuration (see below)
- DNS Settings

The **Switch to Auto Provisioning** link moves you to the Automatic Provisioning page where Quadro can be configured by the automatically provisioning mechanism.

The **Uplink Configuration** page allows to select the Quadro's WAN interface connection type and its bandwidth settings. These settings make Quadro available to the external network.

Depending on the Uplink Interface Protocol selection, the page following the **Uplink Configuration** page is different. Thus if **PPPoE** is selected, the next page will be **PPP Configuration**, while selecting **Ethernet** will bring up the **WAN IP Configuration** page.

The **Uplink Configuration** page offers the following components:

The **WAN Interface Protocol** radio buttons are used to choose the protocol depending on the requirements of the ISP (Internet Service Provider):

PPPoE - turns on the PPP over Ethernet connection type.

PPTP – turns on the Point to Point Tunneling Protocol (**PPTP**) interface used for the connection between Quadro and ADSL modem. Fixed IP address configuration is needed in this case.

Ethernet - turns on the Ethernet connection type.
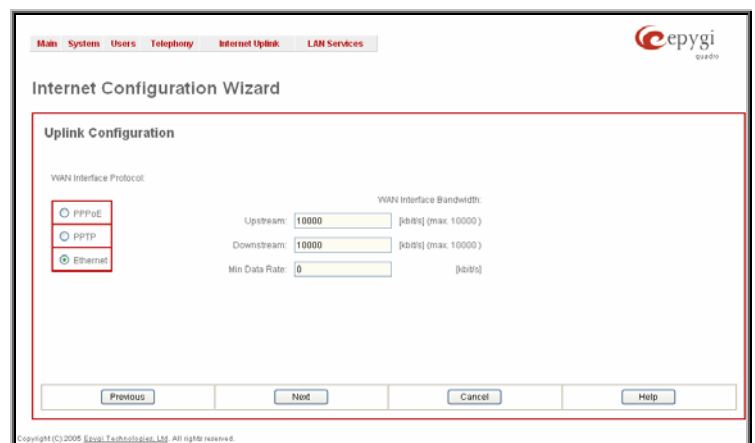
Fig. II-8: Internet Configuration Wizard - Uplink Configuration page

The **WAN Interface Bandwidth** settings allow the specification of the upstream and downstream speeds in kbit/s, helping to assure the quality of IP calls. An IP call looses the voice quality if there will be no available bandwidth. In case of reaching the borders of bandwidth, another IP call will be declined.

The bandwidth provided by the ISP has to be specified in the text fields **Upstream Speed** and **Downstream Speed**. The default entry in both fields is 10000, the maximum bandwidth of a 10 MB Ethernet. But most providers offer a smaller bandwidth than these 10000 kbit/s.

The bandwidth required by an IP call depends on the codecs used and is listed in the tables below:

Required Bandwidth for Standard Packets:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:								
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	G723-5.3	G723-6.3	iLBC-13.33
10	105	58	66	73	81	50	-	-	-
20	84	37	45	52	60	29	-	-	-
30	77	30	38	45	53	22	19	20	27
40	73	26	34	42	50	18	-	-	-
50	71	24	32	40	48	16	-	-	-
60	70	23	30	38	46	15	12	13	60

Required Bandwidth for Encrypted Packets (in the case a VPN is used):

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:								
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	G723-5.3	G723-6.3	iLBC-13.33
10	148	98	105	117	123	92	-	-	-
20	105	59	65	74	80	49	-	-	-
30	91	43	52	60	66	35	33	34	41
40	84	37	45	53	61	29	-	-	-
50	80	33	41	48	56	25	-	-	-
60	77	30	37	46	53	22	19	20	27

The **Min Data Rate** text field requires the amount of upstream bandwidth that ought to remain for data applications even if voice applications use the entire available upstream bandwidth. The value selected here needs to be smaller than the upstream bandwidth and is measured in kbit/s.

The **WAN IP Configuration** page only is displayed if **Ethernet** or **PPTP** has been selected to be the uplink protocol. It offers the following components:

The **Assign automatically via DHCP** radio-button selection switches to automatic retrieval of the WAN IP address from a DHCP server at the ISP/uplink.

Please Note: DHCP refered to here is the one running on the provider's side and not the Quadro's personal DHCP server.

The **Assign Manually** radio-button switches to the manual adjustment of IP settings. This selection requests the following parameters:

IP Address requires the IP address for the Quadro WAN interface.

Subnet Mask requires the subnet mask for the Quadro device WAN interface.

Default Gateway requires the IP address of the router all packets are sent to, for example, the router of the provider.

Fig. II-9: Internet Configuration Wizard - WAN IP Configuration page

The **WAN Interface Configuration** page may be used to modify the MAC address of the Quadro. This might be necessary, if the ISP (Internet Service Provider) requires a certain MAC address, for example, for authentication. The page offers the following components:

MAC Address Assignment manipulation radio-buttons:

- **This Device** turns to the default MAC address of the Quadro.
- **User Defined** requires user defined MAC Address.

MTU drop down list allows to select the maximum packet size on the Ethernet (in bytes). MTU is used to fragment the packets before transmitting them to the network. MTU preferred value is dependent on the Ethernet connection type. The default MTU size is 1500 Bytes for Ethernet and 1400 Bytes for PPPoE.

Fig. II-10: Internet Configuration Wizard - WAN MAC Address Configuration page

Status

The system status window displays non-editable tables providing extensive status information about Quadro: General Information, Network Status, Lines Status, Memory Status, Hardware Status and SIP Registration Status. The links on this page lead to device Transfer Statistics, user mailboxes and supplementary services configuration pages.

The **System Status** page has several tables providing system information.

General Information

The **General Information** page includes the following information:

- **Uptime duration -** Period Quadro is on since last reboot.

- **Device Hostname -** Quadro device host name.

- **Quadro Operating System -** Quadro operating system version.

- **Application Software -** Software and file system versions of the Quadro.

- **Boot Loader -** Quadro boot loader version.

- **DSP Software -** Quadro DSP software version and the date of build.

- **Preinstalled Languages** – field is present only when multiple languages are preinstalled on the device and indicates the system default languages.

- **Language Pack** – field is present only when custom language pack is uploaded and indicates its version.
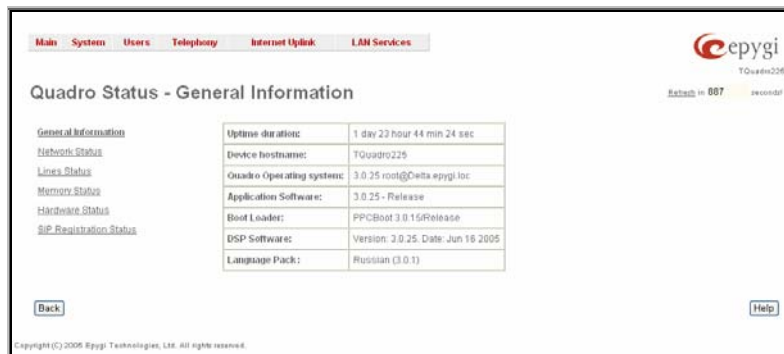
Fig. II-11: Quadro Status - General Information page

Network Status

The **Network Status** page includes the following information about **Interfaces**:

Interface Name lists the Network interfaces available on the Quadro (LAN, WAN, IPSec and a number of PPPs, depending on the number of active PPP connections).

IP Address lists the IP addresses corresponding to each network interface.

Subnet Mask lists the subnet masks corresponding to each network interface.

Properties lists either the MAC address corresponding to each network interface on the Quadro or PPTP, L2TP and IPSec peer IP address if an active VPN (IPSec or PPP) interface exists.

Monitor includes links to survey LAN, WAN, IPSec and PPP traffic correspondingly. The VPN traffic link will be displayed only if a VPN has been configured. The selection of these links will open a new window with a table of network traffic statistics on the selected interface:

Fig. II-12: Quadro Status Network Status page

- Received Bytes
- Transmitted Bytes
- Received Packets
- Transmitted Packets
- Received Errors
- Transmitted Errors
- Received Drop Errors
- Transmitted Drop Errors
- Received Overrun Errors
- Transmitted Carrier Errors
- Received MultiCast Packets
- Transmitted Collisions

When opening the corresponding interface statistics window, no traffic values are displayed at first. Then every one minute, traffic statistics will be updated. The tables serve as a kind of counter.

DNS Server, **Alternative DNS Server** and **Default Gateway** - displays the Quadro settings corresponding to what has been configured with the System Configuration Wizard.

Services (NTP Server and Client, DHCP Server and Client, DNS, Firewall, NAT, PPP) statuses: **stopped** or **running**.

View VPN Status link refers to the VPN Configuration page where all VPN (IPSec, PPTP and L2TP) connections can be viewed and edited.

Transfer Statistics - link to the Transfer Statistics page.

The **Transfer Statistics** page allows a user-defined statistic table depending on the transmit/receive value (criteria), interface type and time period. It contains the following components:

Time Range of statistic table - the drop down list includes the period(in days) statistics data is to be collected and the corresponding diagram charts are to be built.

Interface - the drop-down list offer the values:

- **WAN** - Wide Area Network (WAN) events only
- **LAN** - Local Area Network (LAN) events only

When **Show also as readable values** checkbox is selected, an additional table with statistics values will be displayed on the next page.
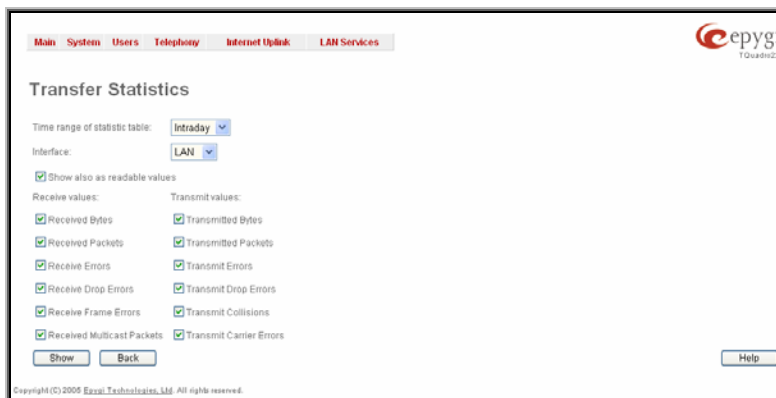
Fig. II-13: Transfer Statistics page

The area **Receive Values**:

- **Receive Bytes** - number of received bytes
- **Receive Packets** - number of received Ethernet packets
- **Receive Errors** - number of received packets containing errors
- **Receive Drop Errors** - number of received packets that have been discarded
- **Receive Overrun Errors** - number of received overrun errors that occur when the receive buffer is not large enough to hold all incoming packets. This error mostly appears because of a slow receiving system.
- **Receive MultiCast Packets** - number of received broadcast packets

The area **Transmit Values**:

- **Transmit Bytes** - number of transmitted bytes
- **Transmit Packets** - number of transmitted Ethernet packets
- **Transmit Errors** - number of transmitted packets containing errors
- **Transmit Drop Errors** - number of transmitted packets that have been discarded
- **Transmit Carrier Errors** - number of transmit carrier errors that occur because of a defective or lost connection on the Ethernet link
- **Transmit Collisions** - number of transfer errors that occurred during a simultaneous packet transmission from both sides
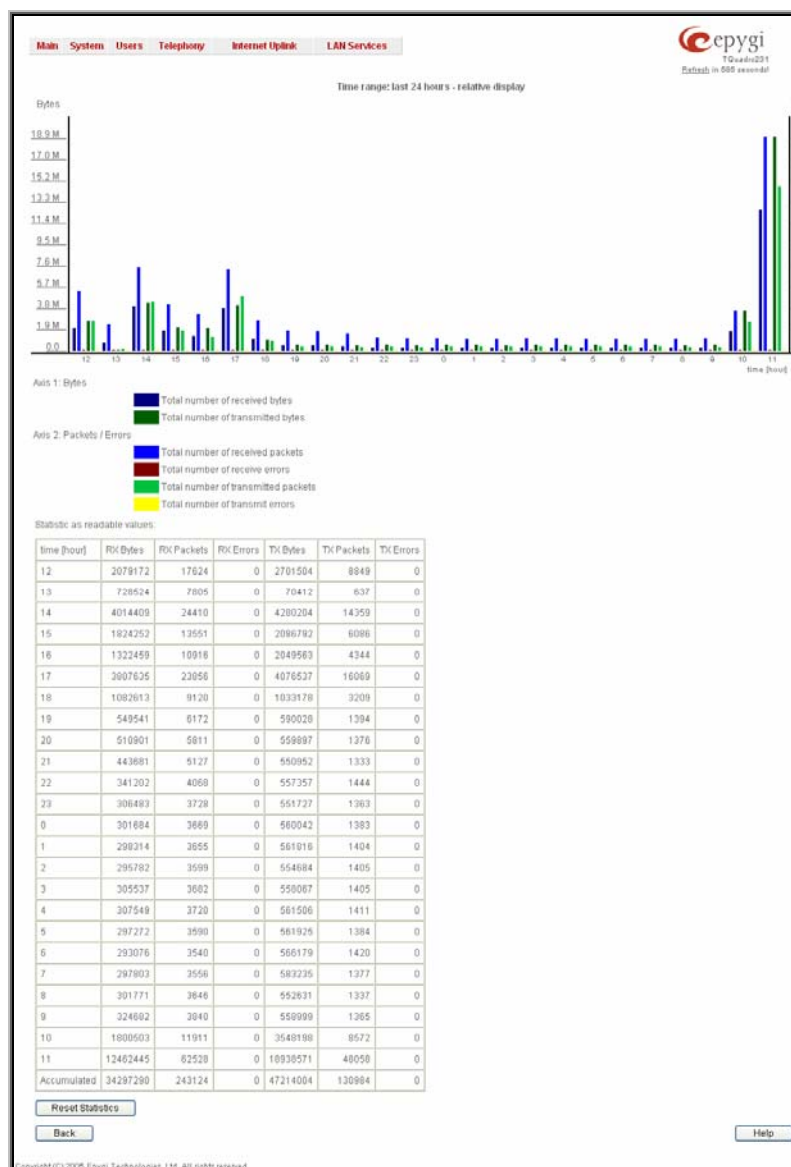
Fig. II-14: Transfer Statistics Diagram Chart

To show the **Transfer Statistics Diagram Charts**, select the desired criteria and click **Save** to generate the corresponding chart and the table with transfer statistics values (if enabled). The letters **M** and **K** used in the legend of the displayed diagrams show the total number of specified criteria: **K** means thousands and **M** millions. **Reset Statistics** button is used to reset the chart and the table (if enabled).

Lines Status

The page **Quadro Status** - **Lines Status** shows the current status of each of the FXS, IP and FXO lines with all details of the attached extension. Since only one line of information can be displayed at a time, the **Line, IP Line** and **FXO** functional buttons are used to navigate through the other lines' information.

The **Lines Status** table displayed for **FXS** and **IP** lines include a group of static and dynamic parameters. Static parameters are displayed, always, while dynamic parameters only appear whenever an event takes place on the extension.

Static Parameters:

Extension shows the extension number of the selected telephone line.

Display Name shows the corresponding name.

Phone State may have the value **on hook** or **off hook**.

Number of Active Calls shows the number of calls that are currently present on the phone.

Dynamic Parameters:

Call State shows the current state of the extension (in voice mail, in call, waiting, busy, call out, ring in, etc.).

Caller Party appears whenever a call is received and indicates the caller extension and the IP address or a phone number, depending on the call type.

Called Party appears whenever a call is placed and indicates the destination extension and the IP address or a phone number, depending on the call type.

Call Type shows whether the call is **Internal** or **External** and whether it is a **PSTN**, **PBX** or an **IP Call.**

Call Start Time shows the call start date and time.

Call Duration shows the current call duration.

RX Codec shows the codec used to encrypt the incoming packets. **TX Codec** shows the codec used to encrypt the outgoing packets. If RX and TX codecs are the same, one **Codec** field will be displayed instead.
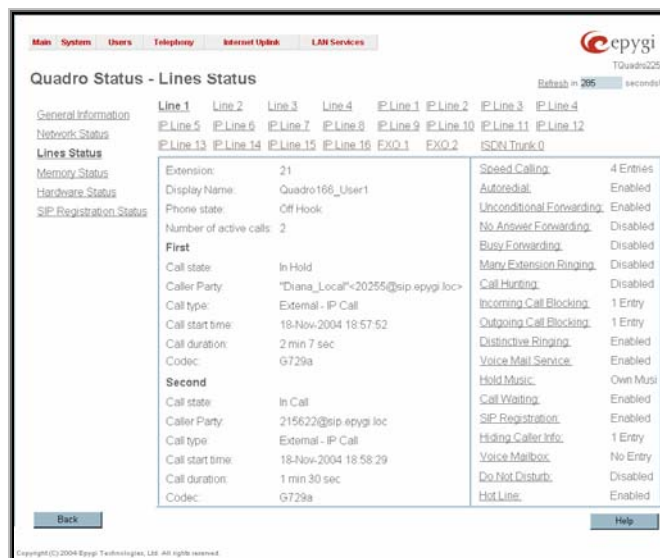
Fig. II-15: Lines Status - Line Status page upon established call

There is a list of supplementary services with their statuses for each telephone line: **Enabled**, **Disabled** or -in case of the services **Incoming** and **Outgoing Call Blocking**, **Speed Calling**, **Hiding Caller Info** and **Voice Mailbox** - the number of **Entries** in the corresponding service table. Thus the administrator may follow and will be notified about services running on Quadro for every line. The services are designed as links that guide the administrator to the corresponding service page of the selected user.

Fig. II-16: Quadro Status - Lines Status

The **Lines Status** table of each **FXO Line** gives information about the **Allowed Call Types**, shows the extension number (attendant or routing client), shows to whom the **Incoming Call** is **Routed To** and displays the **State** of the line (**Free** or **Busy**).
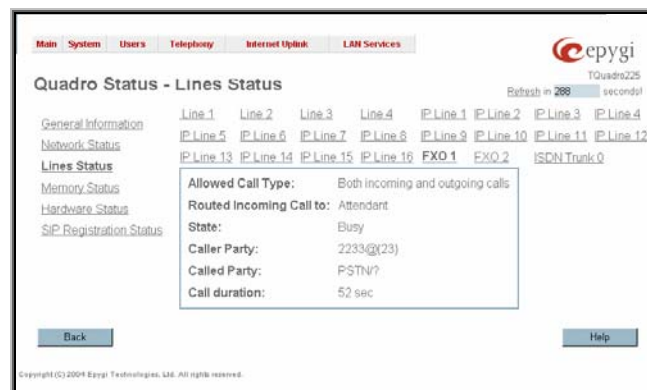
Fig. II-17: Line Status - FXO Status page

The **Line Status** for **ISDN Trunk** displays the state of the B1 and B2 channels and the information about the active calls on them. The page includes a group of static and dynamic parameters. Static parameters always are displayed, while dynamic parameters appear only whenever an event takes place on the channel.

Static Parameters:

- **B channel** - the state of the channel (enabled or disabled)
- **State** - the current state of the channel (free, busy or N/A)

Dynamic Parameters:

- **Caller Party** - this parameter appears whenever a call is received and indicates the caller address
- **Called Party** - this parameter appears whenever a call is placed and indicates the destination address
- **Call Duration** - current call duration
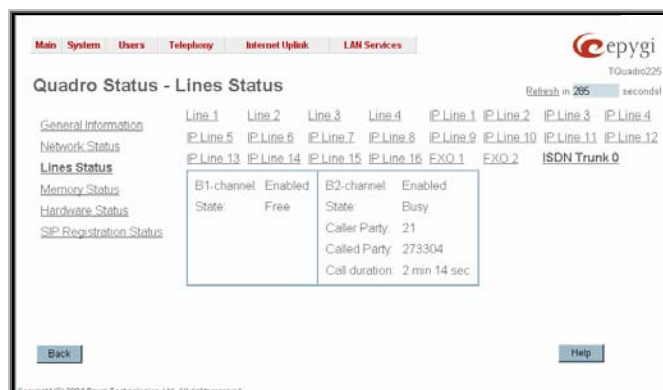
Fig. II-18: Lines Status page

Memory Status

The **Memory Status** page includes tables with the available **User Space** information for each extension. These tables display the space used by the voice mailbox and uploaded/recorded system greetings, and the free and total space (counted in minutes/seconds) for every extension. The page includes the following information:

Memory Size shows total memory space (counted in minutes/seconds) available on the Quadro and assigned to all extensions.

The table's links lead the administrator to the extension settings page where **User Space** may be altered.

System Memory row indicates the space occupied by the universal extension recordings. Link refers to the Upload Universal Extension Recordings page where universal extension system messages may be uploaded.

Call Statistic shows the current number of call statistic entries.
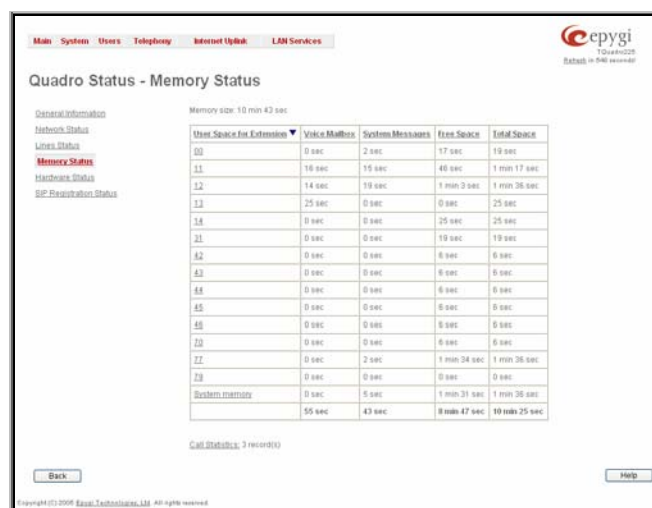
Fig. II-19: Memory Status page

Hardware Status

Fig. II-20: Hardware Status page

The **Hardware Status** table displays a list of the hardware devices present and currently available on the Quadro board. The hardware device version number and additional comments about its state are indicated here.

SIP Registration Status

Fig. II-21: SIP Registration Status page

The **SIP registration Status** is a table displaying the SIP registration status of the Quadro extensions.

The table contains a list of all the registered extensions of Quadro, information about SIP registration states for them, addresses of SIP servers where they are registered (if so), registration date and time, as well as SIP registration names. By clicking on the row heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed next to the column heading.

The links inside the table link you to the <u>Extensions Management</u> page where the SIP registration settings may be altered.

The **Detected Connection Type** field displays the connection type Quadro currently is acting in (direct connection or behind NAT). If Quadro is acting behind NAT, the NAT machine IP address is also displayed.

Registered IP Lines table lists the IP lines and remote extensions registered on the Quadro. Table indicates the actual IP addresses of the remote devices, the usernames by which the devices have been registered on the Quadro, as well as the registration status information.

IP Routing Configuration

Routing is used to relay information across the Internet from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing is often confused with bridging, which may seem to accomplish precisely the same thing to the casual observer.

Quadro's **IP Routing** service allows to route IP packets from one destination to another (or to a specified router) through Quadro or a Quadro VPN.

The **IP Routing Configuration** page is used to make IP Static, IP Policy and VPN routes for IP packets routing and has three tables. Entries in the tables are colored according to the state of the route, i.e. yellow for disabled routes, green for successfully enabled routes and red for erroneously enabled routes.

IP Static Routes are used to forward IP packets from the Network, where the Quadro is connected, to the specified destination.

The **IP Static Routes** table displays all established IP static routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Route To** for the subnet where the incoming packets should be routed and **Via IP Address** for the router IP address incoming packets should be routed through.

Add opens the **Add IP Static Route** page where a new static

route can be established.

Enable/Disable are used to activate/deactivate selected route(s). At least one route should be selected in order to use these functions, otherwise the error message appears: "No record(s) selected."

The page **Add IP Static Route** offers the following components:

Route To requires the IP address and subnet mask of the destination the IP packet ought to be forwarded to.

Via IP address requires the IP address of the subsequent router for IP packet forwarding to the specified destination.

Attention: The rule with the longest subnet (smallest IP range) will take effect when having two or more IP Static routing rules with the coinciding subnets.

Fig. II-23: Add IP Static Routing page

IP Policy Routes allow IP packets forwarding to the specified router depending on the source IP address as well as defining the priority for the current routing rule.

The **IP Policy Routes** table displays all specified IP policy routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Priority** for the route priority, **Route From** for the subnet, routed packets come from and **Via IP Address** for the router IP address incoming packets should be routed through.

Add opens the page **Add IP Policy Route** to establish a new policy route.

Enable and **Disable** are used to activate or to deactivate the selected route(s).

Raise and **Lower Priority** are used to increase or to decrease the priority of the selected policy route(s) by one. At least one route should be selected to use these functions, otherwise the error message appears: "No record(s) selected."

Fig. II-24: IP Policy Routing table

The page **Add IP Policy Route** offers the following input options:

Priority requires a numeric value (from 1 to 252) to define the priority of the routing rule. The lower the number, the sooner the routing rule will take effect (higher priority).

From requires the packet source IP address and subnet mask of the specified destination to match with the rule.

Via IP address requires the IP address of the subsequent router for IP packet forwarding.

Fig. II-25: Add IP Policy Route page

The **VPN Routes** allow IP packets forwarding through the PPTP and L2TP tunnels of the Quadro. If no PPTP/L2TP connections exist on Quadro, no VPN routes can be generated.

The **VPN Routes** table displays all generated VPN routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Route To** for the subnet where the incoming packets should be routed, **Via Tunnel** for the VPN tunnel incoming packets should be routed through and **Tunnel State** for the actual state of the route tunnel (up or down).

The **Add** button opens the **Add VPN Route** page where a new VPN route can be generated.

Fig. II-26: VPN Routing table

The **Add VPN Route** page offers the following components:

Route Via contains the available PPTP and L2TP connections on the Quadro. A connection selected from this list will be used to route the IP packet from the Quadro's LAN to the peer behind the PPTP/L2TP tunnel.

Route To requires the IP address range of the possible peers behind the PPTP/L2TP tunnel whereto IP packets could be routed.
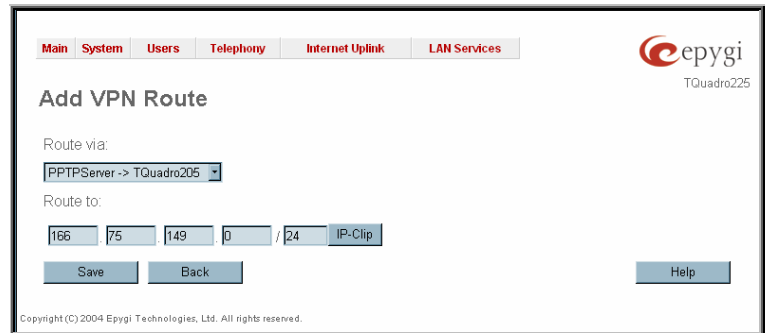
Fig. II-27: Add VPN Route page

The **Enable** and **Disable** functional buttons are used to activate or to deactivate the selected route(s). At least one route should be selected to use these functions, otherwise the error message appears: "No record(s) selected."

To Add an IP Static Route

1. Select the **IP Static Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Static Routes** page. The **Add Entry** page will appear in the browser window.
3. Enter the destination IP address and subnet mask in the **Route To** text fields. Use the **IP-Clip** button to select a previously entered IP address.
4. Enter the router IP address into the **Via IP Address** text fields.
5. Press the **Save** button to make the static route with these settings.

To Add an IP Policy Route

1. Select the **IP Policy Route**s link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Policy Routes** page. The **Add Entry** page will appear in the browser window.
3. Specify the policy routing rule priority in the **Priority** text field.
4. Enter the packet source IP address and subnet mask in the **From** text fields. Use the **IP-Clip** button to select a previously entered IP address.
5. Enter the router IP address into the **Via IP Address To** text fields.
6. Press the **Save** button to make the policy route with these settings.

To Add a VPN Route

1. Select the **VPN Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **VPN Routes** page. The **Add Entry** page will appear in the browser window.
3. Choose the VPN connection from the **Route Via** drop down list.
4. Enter the destination IP address and the subnet mask into the **Route To** text fields.
5. Press the **Save** button to make the VPN route with these settings.

Configuration Management

The **Configuration Management** assists the administrator to manage the system configuration settings and voice data, i.e., to backup and download the settings to the PC and then to upload and restore them back to the Quadro. Additionally this page gives a possibility to restore the factory default configuration settings.

The **Backup & Download all config & voice data** link generates a backup file with all configuration settings and user uploaded greeting messages and opens a file chooser window for immediate download to the user PC.

Attention: Configuration and voice data cannot be backed up if the size of voice data is too large. In this case, to be able to backup configuration and voice data on the Quadro, please remove some user defined system messages (by restoring the default ones, see chapter Update System Messages), or remove some extensions from the Extensions Management table.

Fig. II-28: Configuration Management page

The **Upload & Restore all config & voice data** link opens a page with the **Browse** button, (which opens a file chooser to select a backed-up file) and a **Configuration to Upload** field requiring the file path to upload and to restore it immediately. Pressing **Save** will restore the selected backup file, and delete all current user defined greetings and replace configuration settings.

The **Use Default** functional button resets all configuration settings and restores the board's factory default configuration. By restoring the default configuration you will replace your current one, lose all voice mails and reboot the device. You will not be automatically redirected to the GUI start page. After the successful reboot you will need to enter into the management and login again to access the Quadro's configuration. A warning message will ask you to confirm your selection before restoring the default configuration.

Please Note: Unlike the factory default settings restore procedure initialized from the Reset button on the Quadro board, this link will keep the following data:

- Call Statistics

- Transfer Statistics

- System Events

- Feature Keys

- Device Registration state

Update Configuration link leads to the page where Quadro's configuration can be automatically or interactively update, downloaded and edited.

Update Configuration

The **Update Configuration** allows to automatically or interactively update Quadro's configuration, as well as to download a legible and editable configuration file, make necessary changes and upload it back to the system. This particularly allows to use parts of the configuration of one Quadro on another Quadro with some changes done prior to uploading the new configuration. Service is mainly used by Quadro reseller, distributor, ISP or carrier.

Attention: It is strongly recommended to consult with technical support center before making changes on this page. Incorrect settings here may corrupt current configuration. Page consists of the following components:

Server and **Server Port** text fields require IP address or Host name and the port number of the server configuration will be downloaded from.

Update Method drop down list indicates the connection type used to download the configuration (ftp, tftp, http or https).

Enable Version Check checkbox selection enabled version verification before configuration is being downloaded.

Attention: Disabling **Enable Version Check** checkbox may cause incompatibility problems on the device.

Update Interval Selection manipulation radio-button group is used to select the frequency of configuration check/update performed on the Quadro:

- **Check/Update at boot time** – with this option, new available configuration will be checked/updated each time after Quadro boots.

- **Check/Update manually** – with this option, configuration check/upload will be performed only by manual selection.

- **Check/Update time/date scheduled** – with this option new available configuration will be checked/updated periodically dependent on the selected time and/or weekday. This selection enables **Time Based** and **Weekday Based** checkboxes. Selecting one or both of them allows to define the time and the weekday, when configuration check/update will be automatically performed.

Fig. II-29: Upload Configuration page

Update Policy Selection manipulation radio-button group is used to select the operation performed on the selected:

- **Check only for update** – with this option, system will only perform checking of the availability of new suitable configuration and will log corresponding event in the Events table (depending on configuration in Events Settings).

- **Check and update immediately** - with this option, system will check the availability and correspondingly update the new configuration and will log corresponding event in the Events table (depending on configuration in Events Settings).

- **Check and update immediately without any feedback** - with this option, system will check the availability and correspondingly update the new configuration but will not log any events on this.

Check now for new update functional button performs manual checking of the availability of new suitable configuration and logs corresponding event in the Events table (depending on configuration in Events Settings).

Update now functional button performs manual checking and update of the availability new configuration and logs corresponding event in the Events table (depending on configuration in Events Settings).

Update now without feedback functional button performs manual checking and update of the availability new configuration and does not log any events on this.

Download current configuration in a legible format link refers to the **Configuration Summary** page where necessary configuration part or a complete configuration can be defined and downloaded or viewed.

Configuration Summary page is used to define the necessary configuration part and to download it to PC or to view it directly in the browser.

In the text field on this page configuration part need to be downloaded should be specified. Pressing **Start generate a legible configuration file** will start parsing the configuration structure of the device. Progress will be seen in the area below.

Cancel generation process button appears immediately configuration generation procedure starts and is used to stop it.

Download generated configuration button becomes available once legible configuration generation is over and is used to download the generated file to the PC in the plain text format. Necessary changed can be done in the downloaded configuration file and then uploaded back to the system.

Fig. II-30: Configuration Summary page

Attention: Make sure the changes you have done in the downloaded legible configuration file are valid and will not corrupt the system when being uploaded back to device.

View generated configuration button becomes available once legible configuration generation is over and is used to view the generated file directly in the browser.**Upload a legible configuration file** link refers to the page where configuration file can be uploaded in text format. **Browse** button in the opened page is used to browse the certain legible configuration file to be uploaded and updated to the system. Configuration files to be uploaded should be in the *.txt format, otherwise system error occurs. Configuration file upload progress will be displayed in the area below.

Events

The **Events** page shows two tables and displays all system events that have occurred in one table and event settings in the other.

The **System Events** page may be accessed with **Events** link from the main menu. It lists information about system events that have occurred on Quadro. When a new event takes place a record is added to the System Event table and for failure events (priority 2 and 3, see below) additionally a warning "Please check your pending events!" appears at the bottom of all management pages.

The system events and the warning message are visible only for the administrator. The warning link, (which leads directly to the **System Events** page) will disappear from the management pages if the administrator has marked all new events as read.
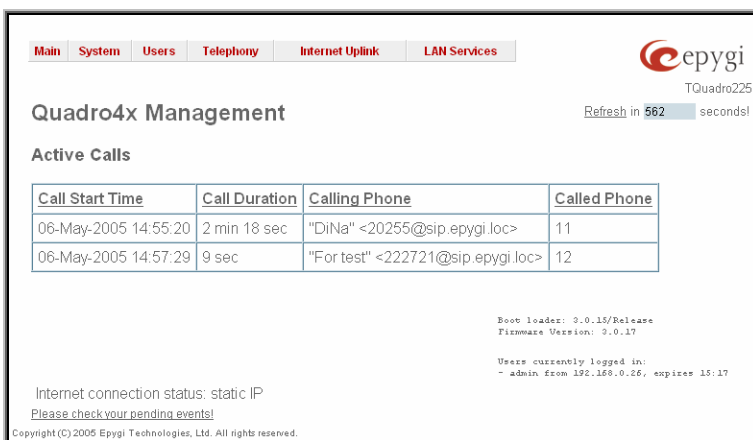
Fig. II-31: Event Warning on the Main Menu page

Fig. II-32: System Events list

The **System Events** table is the list of new and read system events. System events have the corresponding coloring depending on the nature of the event: success (priority 1, color green), low importance failure (priority 2, color yellow), critical failure (priority 3, color red).

The table shows the **Status** of the event (new or read) as well as the name of the application the event refers to, event description, and the date when the event was received. For example, if the event has occurred due to incorrect mail sending or SIP registration, corresponding links will be seen in the Reference column of the table. There the administrator can view the detailed log for the event that has occurred. There the administrator can view the detailed log for the event that has occurred.

The **System Events** page offers the following components:

Current System Time displays the local date and time on Quadro.

Mark all as read marks newly occurred events as read.

Disable LED switches off the LED flashing (if any do flash) on the board. A LED notification may appear (depending on the notification type given) in the page Events settings whenever a new event occurs.

Fig. II-33: Event Configuration Settings page

Numerous circumstances may cause a certain application on Quadro to flag an event.

The page **Event Settings** lists all possible events on the Quadro and allows controlling the way of notification (action), if one of those events takes place.

Each entry in the events' table has its checkbox assigned to the row. By selecting the corresponding checkboxes, operations such as **Edit** may be done for one or more events.

Edit opens the **Edit Event Settings** page to modify the event action.

> **Do Nothing** - Nothing will happen when the event occurs.
> **Display Notification** - A notification link will be displayed on the bottom of all pages and a record is added into the **Events** table. The notification is executed as the link "Please Check you pending events!" that leads to the page **System Events**. This action also will take place if Flash LED or Send Mail has been selected, even if not selected explicitly.
> **Flash LED** - The second LED (yellow) will be blinking once a second and a notification will be displayed on the bottom of all pages. For some events the LED will start flashing after a delay.
> **Send Mail** - An e-mail with a notification about the new event and an event description in the mail body will be sent to the e-mail address specified in the Mail Settings page.

Actions that are not allowed for the selected event (like mail notification if the PPP link is down or the mail server has been misconfigured) are hidden. For multiple events editing, actions that do not fit at least to one of the selected events will be hidden.

If Quadro cannot get an IP address from the DHCP or PPP servers, or cannot register an extension on the SIP or Routing servers, or cannot reach an NTP server, it raises only one event for the entire period the action has failed, but continues to try. When the required action is successful,, Quadro raises an appropriate message.

The page **Edit Event Settings** offers the following input options:

Application displays the application the event refers to. **Multiple** is shown here, if more than one event has been selected for the action assignment.

Name displays the name of the event. **Multiple** is shown here, if more than one event has been selected for the action assignment.

Description displays additional information about the event. **Multiple** is shown here, if more than one event has been selected for the action assignment.

Action offers radio buttons to choose one of the actions to notify the Quadro administrator whenever the selected event(s) takes place.

Fig. II-34: Edit Event Settings page

To Assign an Action to the Event

1.   Select the checkbox of one or more events to assign an action to them.
2.   Press the **Edit** button. The **Edit Event Settings** page appears.
3.   Select an action type from the **Action** radio buttons to notify the administrator about the event in the desired way.
4.   Press the **Save** button to submit the changes or use **Back** to abort the selected action.

Time/Date Settings

The **Time and Date Settings** provide information about the current system time and date. The settings may be updated through the international time and date servers.

Time is used to set the local time (hour, minute).

Date is used to set the date (month, day, year).

Timezone provides a selection of world time zones and is used to select the local country time zone. Timezones are specified by GMT (Greenwich Mean Time) and by specific timezones for the United States and Canada.

Enable Simple Network Time Protocol Server enables the SNTP (Simple Network Time Protocol) server on Quadro, thus Quadro becomes the timeserver for its LAN.

Enable Simple Network Time Protocol Client enables the SNTP client on the Quadro, thus Quadro becomes a client to an external timeserver. The checkbox disables Date and Time drop down lists and enables the following parameters:

The **SNTP Servers** table lists all defined NTP Servers.

Add functional button opens an **Add NTP Server** page where a new NTP server can be defined. This page offers the **NTP Server** radio buttons that are used to choose between a manual and a predefined NTP server.

   Manual requires the NTP server's FQDN (Full Qualified Domain Name) or its IP address.

   Predefined is used to select the NTP server's host address from the drop down list, where the most common NTP servers are listed.

Fig. II-35: Time and Date Settings page

The **Move Up** and the **Move Down** functional buttons are used to sort NTP servers in the order they need to be accessed. If the NTP server on the first position in the **SNTP Servers** table does not answer, NTP server on the next position will try to be reached.

Please Note: Add another NTP server to the list if you feel defined NTP servers are not functional, i.e., the Quadro's date/time is not being updated automatically.

Polling Interval indicates the time interval for the periodical synchronization between timeserver and Quadro. It counts in hours.

Fig. II-36: Add NTP Server page

Attention: Time and Date Settings will be reset if Quadro has lost power.

Mail Settings

The **System Mail Settings** page gives a possibility to send warnings automatically about the board status or problems to the administrator. System events that require email notification are selected on the Events page. Besides, system mail has to be enabled and the SMTP server needs to be configured for voice message transmission to the extension user's mailing account.

Enable enables the system mail sending possibility and voice messages transmission to the extension user's mailbox.

SMTP Host requires the SMTP host IP address or domain name. The SMTP host needs to be configured to enable voice message transmission.

Mail Sender Address requires the source address for the Quadro notification emails. The email address defined here should be an existing valid email address registered on the selected SMTP server or should have permission to use that particular SMTP server for emails transmission.

Mail Recipient Address requires an active email address. The e-mail recipient here can be a Quadro administrator or someone responsible for network and system problems.

Enable SMTP Authentication has to be selected if the specified SMTP server requires an authentication. In this case, authentication **User Name** and **Password** configured on the SMTP server should be defined in the corresponding text fields.

Send Test Mail is used to initiate a test e-mail transmission. This button will be enabled if correct values have been submitted and saved on this page.
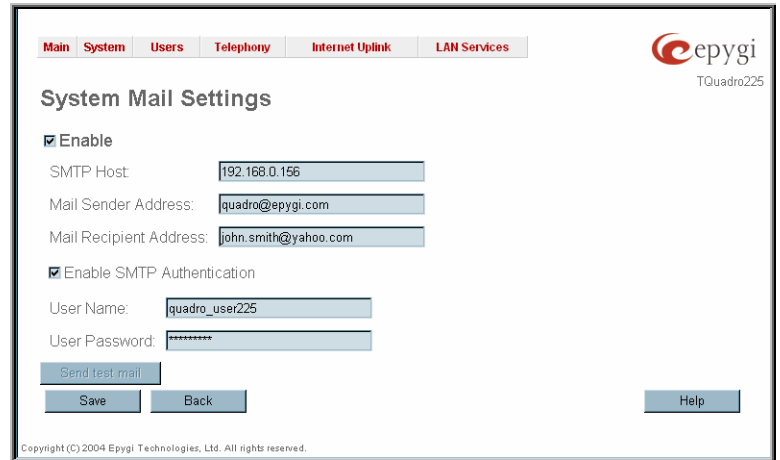
Fig. II-37: System Mail Settings page

To configure the System Mail

1. Enable the system mail sending by the **Enable** checkbox selection.
2. Update or set the SMTP host in the **SMTP Host** text field.
3. Update or set the e-mail sender address in the **Mail Sender Address** text field.
4. Update or set the e-mail address in the **Mail Recipient Address** text field.
5. Enable **SMTP Authentication** if it is required of the server.
6. Insert into the corresponding text fields an authentication **User Name** and a **User Password** defined by your SMTP server.
7. Press the **Save** button to submit these settings.
8. Use the **Send Test Mail** button to send a test e-mail with the configured settings.

SMS Settings

The **SMS Settings** are used to configure the SMS parameters that will allow Quadro to send the voice mail notifications via SMS to the extension user's mobile phone. Every extension user is free to enable the voice mail notifications upon new voice mail arrival and to define own mobile numbers from the Voice Mail Settings. However, to make Quadro able to deliver SMS notifications, SMS service should be enabled and SMS settings should be configured from this page.

Enable SMS Service enables the SMS service on the Quadro.

User Name and **Password** text fields require the authentication settings of the SMS server.

SMS Sender Address requires the source address for the Quadro notification SMS. The address defined in this field will be seen in the "From" field of the SMS delivered to the mobile phone.

SMS Recipient Address requires a destination mobile number for a test SMS.

HTTP Parameters:

> **ID** text field requires an identification number defined by the SMS server.

> **Server** text field requires an IP address or the host name of the SMS server.

> **Port** text field requires a HTTP port number of the SMS server.

> **Use Secure HTTP** checkbox enables access to SMS server via HTTPS. Checkbox selection enables a **Secure Port** text field that requires the port number for HTTPS traffic.
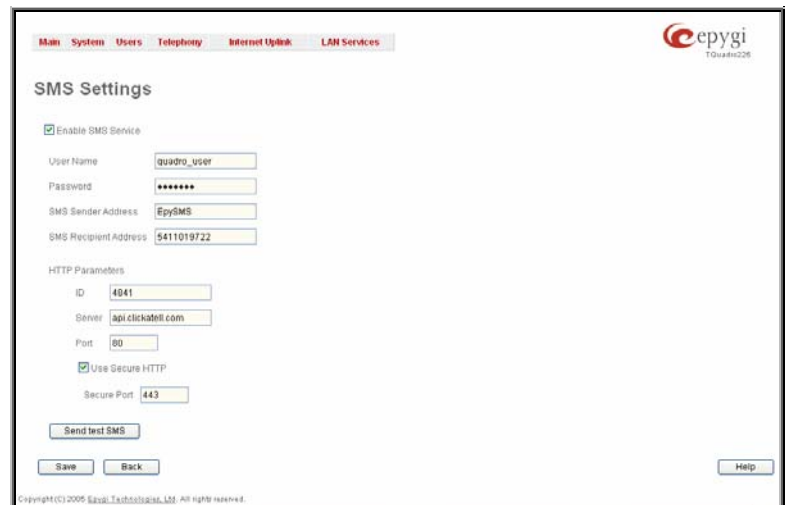
Fig. II-38: SMS Settings page

Send Test Mail is used to send a test SMS to the defined SMS Recipient Address. This button will be enabled if correct values have been submitted and saved on this page.

Firmware Update

This window allows to update the software of Quadro by installing new firmware called image. Users registered at Epygi will receive a notice when new firmware is available and will be able to download it from the Epygi Technical Support WEB page.

Updating a new firmware requires a perfectly working power supply. Therefore Quadro is provided with a battery (accumulator). If the battery is low or simply absent the "There is no battery or voltage is low" warning is displayed

Please Note: Installing new firmware will take about 15 minutes. During this time, the QuadroCS, telephony and Internet access will be disabled.
The firmware update will cause the loss of the following data:

- All internally stored voice mails and custom voice messages
- DHCP leases
- Transfer statistics
- Call statistics
- All pending events
- User specific GUI states

The following main processes will be stopped during the firmware update and will be restarted afterwards:

- Voice Software
- Network Time Protocol Daemon
- Network Interface Statistic Daemon
- Dynamic DNS Daemon

Please Note: If you consider the Call Statistics entries in the displayed tables to be important, it is recommended to download them from the corresponding page prior to starting the Firmware Update.

Next will move you to the second page of Firmware Update where the image file should be selected.
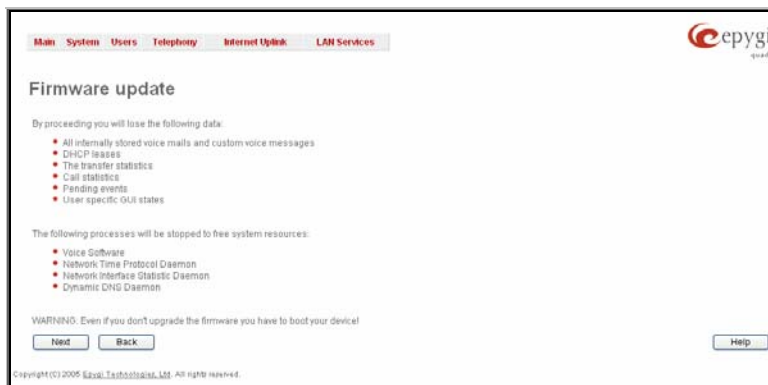
Fig. II-39: Firmware Update page 1

The second page of **Firmware update** has the **Browse** button used to browse the image file, and the **Specify Image** text field that will display the selected image filename.

Pressing **Save** will start uploading the image file to the board. The next page will be displayed, showing the result of a verification of the image being burned.
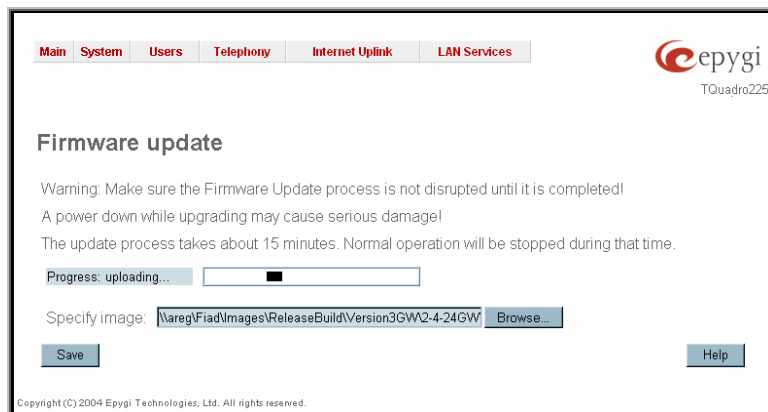
Fig. II-40: Firmware Update page 2

This page displays non-editable information about the image validity. The **Image Check** will display invalid if the image does not correspond to the hardware version.

The fields **Current Software Version** and **New Software Version** show the old software version and the version of the new image.

This page needs a confirmation to continue image updating. If you are sure that the image version is appropriate for your device press **Save**.

Fig. II-41: Firmware Check page

Networking Tools

The **Networking Tools** provide the possibility to check the Internet connection.

Ping sends four ICMP (Internet Control Message Protocol) requests with a default size of 64 bytes to the destination (IP address or host name) specified in the text field **Ping Target**. The response times are logged, and the round trip time (the time required from being sent until being received again) is measured. The results are displayed in the lower area of the page: The minimum and maximum round trip time and its average, the percentage of lost and of received frames.

Traceroute checks the Internet connection by triggering the routers (hops) that are passed to reach the destination specified in the text field **Traceroute Target**. Trace routing gives feedback on the routers passed by packets on the way toward the destination and the round trip delay of packets to these routers.

Attention: No **Traceroute** is possible if a high priority Firewall has been enabled (see chapter Firewall and NAT).

For the purpose of tracerouting, several IP packets are sent out. UDP (User Datagram Protocol) is used to send packets and ICMP (Internet Control Message Protocol) is used to receive information about the routers. In their headers, the TTL (Time To Live) value increases from 1 to 30. When the first IP frame is received by the first router, its IP address will be returned in its acknowledgement

The second frame delivers the IP address of the second router and so on and so forth. The results of **Traceroute** are displayed on the lower area of the page.
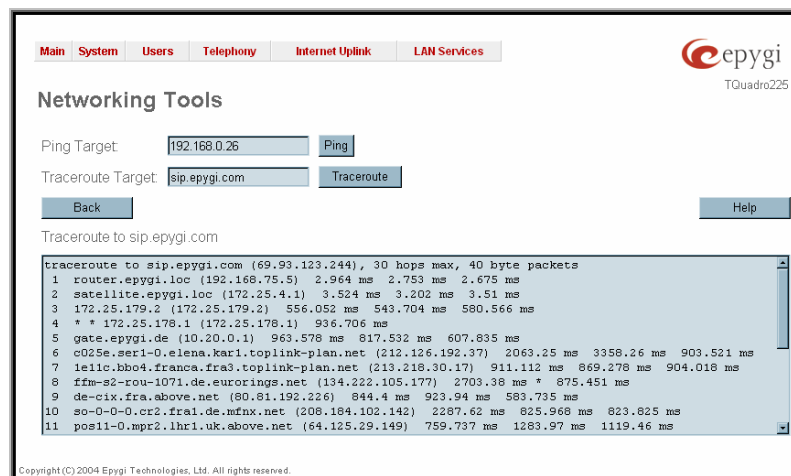
Ping Target requires the destination (IP address or host name) for the ICMP request.

The **Ping** button starts pinging the specified ping target.

Traceroute Target is used to enter the IP address or host name of the destination to be trace routed.

The **Traceroute** button is used to process the router triggering to check the Internet connection.

In the field below the output of the Ping or Traceroute procedure is shown.

Fig. II-42: Networking Tools page

To Check the Internet connection

1.   Specify destination address for the ICMP request in the **Ping Target** text field.
2.   Press the **Ping** button to process the ICMP request.
3.   Specify the destination address to trace the route.
4.   Press the **Traceroute** button to process the router triggering.

Diagnostics

The **System Diagnostic** page gives a possibility to run Network and WAN protocol diagnostics, to verify Quadro's connectivity and to download all system logs for possible problems recovery.

The **Start Detecting WAN Protocol** button is used to initiate WAN diagnostics that will detect the WAN IP configuration: static or through DHCP and PPP servers. For static WAN IP configuration, gateway availability is checked. When acting as a client, DHCP and PPP servers' accessibilities are being verified.

The **Start Network Diagnostics** button is used to initiate network diagnostics, i.e., to check the WAN link and IP configuration, to verify gateway, DNS primary and secondary (if configured) servers' accessibilities.

The **Start ISDN Diagnostics** button is used to initiate ISDN BRI low level diagnostic. With these tests ISDN physical link is checked and Frame Synchronization is verified.

The field below will display the diagnostics results and the connectivity conditions. The system should be reconfigured if problems occur during the diagnostics.

The **Download system logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that had occurred on your Quadro.

The **Reboot this Device** button is used to reboot the Quadro. Please note that the session with the Quadro will be closed, i.e., the Quadro GUI should be newly opened and a new login will be required afterward.

Fig. II-43: System Diagnostic page

Automatic Provisioning

Automatic Provisioning gives a possibility to automatically configure the WAN network settings of Quadro. This is very useful, when the administrator is not actually aware about the Quadro's network settings. **Automatic Provisioning** automatically detects the matching network configuration settings and by applying them on the Quadro, it connects the device to the internet through the available ISP connection.

Please Note: Automatic Provisioning can be run only from the LAN side of the Quadro, i.e. from the PC connected to the Quadro's LAN.

Automatic Provisioning automatically detects and configures the following settings on the Quadro:

- WAN interface type (PPPoE or Ethernet)
- WAN IP settings
- PPP settings
- ISP settings
- DHCP settings
- DNS settings
- NAT Traversal settings
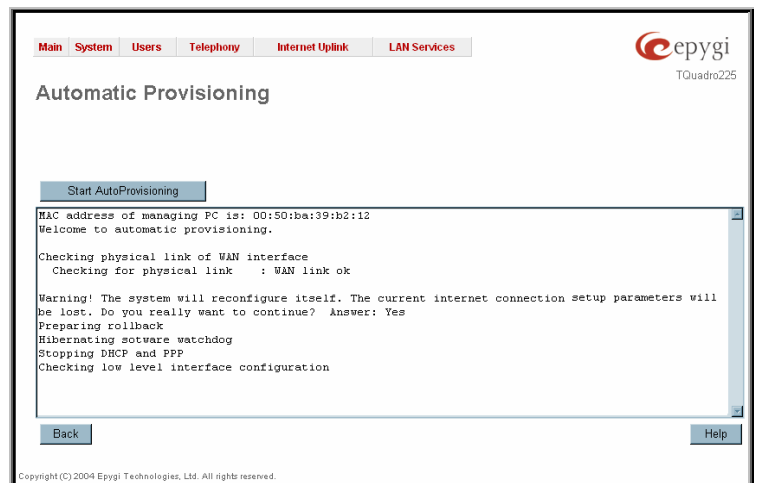
Fig. II-44: Auto Provisioning page

Features

This page lists all features, that may be activated by a software key, characterized by a **Feature Description** and provided with its **Status:**

- **No Key Found** - the feature is currently not available
- **Reboot Needed** - the feature key has been entered and Quadro has to be rebooted
- **Activated** - the feature is available

Following features may be activated via the software key:

- **IP Phone support** - enables additional 4 LAN-sided IP phones on the Quadro.
- **Debug** – enabled Telnet connection towards the Quadro for debugging purposes.

To enter a **Feature Key** click **Add**. A page with the text field **Feature Key** is opened. Enter the key and press **Save**. The status of the selected feature entry will change to **Reboot needed**. Reboot the Quadro and the feature will get the status **Activated.**

To get a **Feature Key** register the Quadro device and send a corresponding request to Epygi's Technical Support. This request must include the **Unique ID** that is displayed in the **Features** page above the features list.

Fig. II-45: Features page
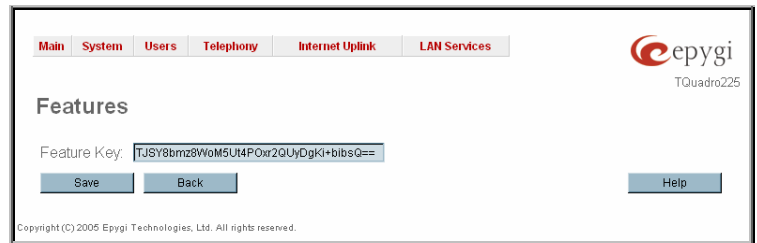
Fig. II-46: Features Add page

Upload Language Pack

Upload Language Pack page allows to upload a custom language for GUI and Voice Messages of the Quadro. The language of voice messages can be switched to the custom Language Pack language from GUI setting page at the System Configuration Wizard. The language of GUI session can be changed to the custom Language Pack language from the radio buttons on the login page.

Uploading a Language Pack will cause the loss of the following data:

- All internally stored voice mail
- DHCP leases
- Call statistics
- Pending events
- Transfer statistics

Please Note: Only one custom Language Pack can be uploaded at the time. Uploading a Language Pack will remove the existing one (if existing) and will reboot the Quadro.

Fig. II-47: Upload Language Pack page

Current Language Pack field displays a read only information about the custom language pack uploaded. When no custom language pack is uploaded, field indicates "unknown".

Below, there is a **Language Pack File to Upload** text field which displays the selected image filename. **Browse** button is used to browse the custom language pack to be uploaded.

Remove Current Language Pack link is seen only when custom language pack is uploaded and is used to remove it from the system.

Pressing **Save** will start uploading the custom language pack to the board. The next page will be displayed, showing the result of a verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if any).

After final confirmation, system will upload the selected custom Language Pack and will reboot.

User Rights Management

User Rights Management service is used to set restrictions on the GUI access for various users, to permit or deny the access to certain Web GUI configuration pages and to create a multilevel user management of the Quadro. Feature is mainly useful to the ISPs to set the restrictions for certain customers to manage the Quadro's configuration.

Two levels of Quadro GUI administration are available:

- **Administrator** – this is a main (super) administrator's account. It is a matter of configuration whether to have password factory reset safe or not, i.e. whether default password will be retrieved after the factory reset or not. Administrator has an access to all Web GUI pages, no configuration permissions can be adjusted for this account. Administrator is responsible for granting access to all other user groups.

- **Local Administrator** – this is a common (sub-) administrator's account. Password is not factory reset safe. Local Administrator's permissions can be adjusted per each GUI page.

- **Extension** – account refers to all extensions created on the Quadro. The password for default extensions is not factory reset safe but is contained in the backed up configuration. Extension's permissions can be adjusted per each GUI page.

User Rights Management page consists of two pages: **Users**, no manage the available users on the Quadro, and **Roles**, to assign the corresponding permissions to the users.

Users page contains a table where Administrator and Local Administrator users are listed. Page allows to modify the passwords of available users in the table and to manage the Local Administrator's account. Following functional buttons are available on the page:

Change Password functional button is used to change the password of the Administrator and Local Administrator user's account. Select one of the available users in the table by toggling the corresponding checkbox and press **Change Password** to open the corresponding page.

Fig. II-48: Users page at User Rights Management

The **Change Password** page is used to change the user's password. It offers the following components:

Old Password text field is only present when modifying the Administrator account password and requires the current password of Administrator. An error message prevents from entering a wrong one.

New Password requires the new password for Administrator or Local Administrator, which has to be confirmed in **Confirm New Password**.

The password may consist of numerical values only, up to 20 digits are allowed. A corresponding warning appears if any other symbols are inserted.

Store password in persistent area (Factory reset save) checkbox is only present when modifying the Administrator account password and is used to save the Administrator's in the factory reset safe place.

Attention: Be EXTREMELY careful when enabling this checkbox – if it is done, Administrator's password won't be retrieved even after factory reset. In this case, if Administrator's password has been forgotten, the Quadro will be considered as broken. Please contact Epygi Technical Support Center for device replacing.

Fig. II-49: Change Password page

Enable User and **Disabled User** functional buttons are used to enable/disable the Local Administrator's account.

Please Note: Administrator's account cannot be disabled.

Fig. II-50: Roles page at User Rights Management

Roles page contains a table where Local Administrator and Extensions users are listed. Page allows to set the permissions to the GUI pages for each user in the table.

Edit functional button leads to a **Change Access Rights** page where a list of user specific GUI pages is displayed. Select on of the users in the table and press **Edit** to manage the permission for the corresponding user.
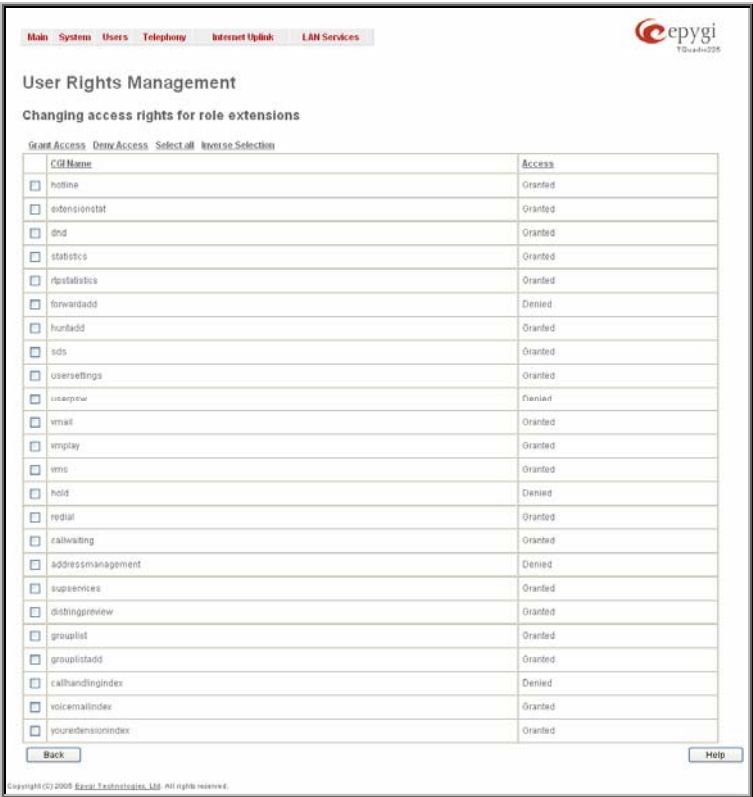
Fig. II-51: Edit Roles page at User Rights Management

On the **Change Access Rights** page, **Grant Access**/**Deny Access** functional buttons are used to grant/deny the access to the certain GUI page(s) for the selected user.

When the access to the certain GUI page is denied for a user, "You are not authorized to access this page!" warning message will be displayed when user attempts to open the corresponding GUI page.

Users Menu

Fig. II-52: Telephone Users Menu in Dynamo Theme

Fig. II-53: Telephone Users Menu in Plain Theme

Extensions Management

The **Extensions Management** is used to create user extensions and auto attendants on the Quadro. From this page, by clicking on the user extension, administrator can get the extension settings pages.

Two types of user extensions can be created on the Quadro: **active** and **inactive** extensions. Active extensions are those that are attached to a line, can place and receive calls and use available telephony services. Inactive extensions are those that are not attached to the line, they can use some available telephony services but cannot place and receive calls; instead, they have a voice mailbox available to keep the brief messages from the callers.

Quadro2x has two available lines and up to two active extensions can be established.

Attendant extensions are dedicated to the IVR system on the Quadro, which is used by the callers to reach Quadro's users, use remote access and call relay services. It is possible to create Auto Attendants with the custom scenarios. By default, Quadro has one Auto Attendant extension (00) which is undeletable.

The **Extensions** table is a list of all extensions and their parameters.
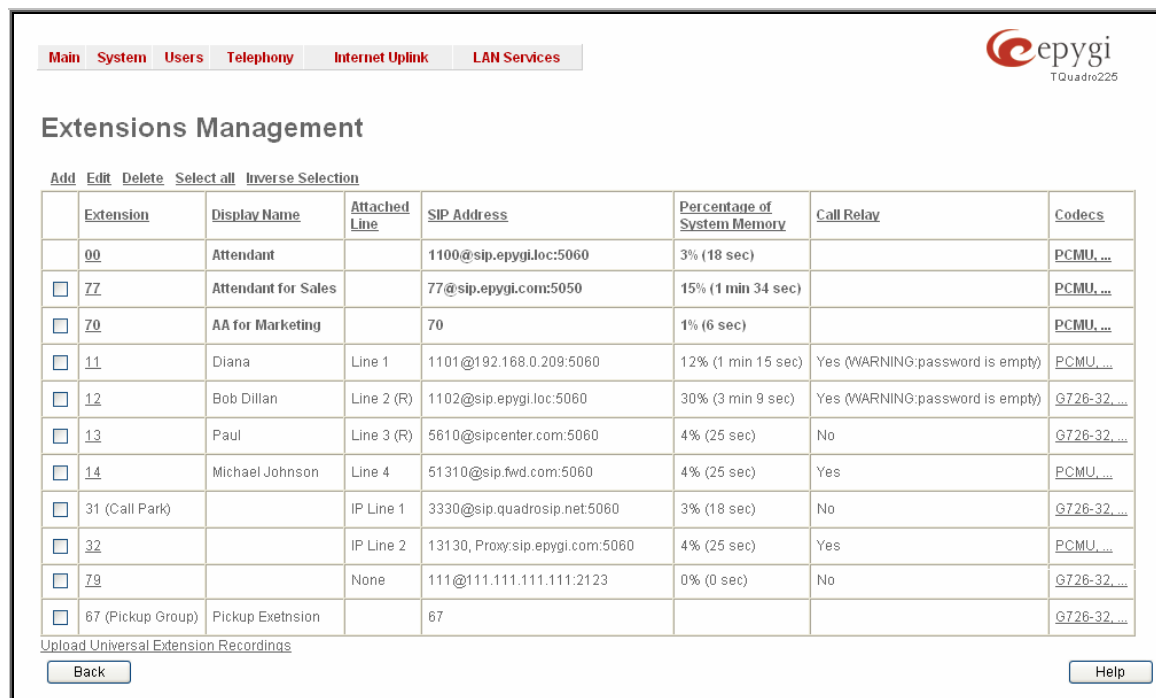
Fig. II-54: Users Management page

The following columns are present in the table:

- **Extension** - lists the 2-digit user or attendant extensions on the Quadro. This number is used for internal PBX calls.

- **Display Name** - indicates an optional display name to identify the caller.

- **Attached Line** - indicates the FXS or IP line corresponding extension is attached to. "R" is displayed in this column when **SIP Remote Extension** (see below) functionality is enabled on the extension.

- **SIP Address** - displays the SIP address of the corresponding extension. Column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. Else, if registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will be skipped in this column. If no username is defined, the extension number will be displayed instead.

- **Percentage of System Memory** - indicates the user space (in percent) configured for each extension. The actual available duration (in minutes) for the extension voice mails, uploaded/recorded greetings and blocking messages is also displayed herein. The available minutes corresponding to the selected user space are dependent on the Voice Recording codec selected from the Voice Mail Common Settings page, for example, for the same amount of marked out user space, selection of the G726 voice recording codec will provide more space for voice mails and user defined voice greetings than the G711 codec selection.

- **Call Relay** - indicates whether or not Call Relay option is enabled on the extension.

- **Codecs** – column lists the short information (full information is seen in the tool tip) about extension specific voice Codecs. Extension codec's can be accessed and modified by clicking on the link of the corresponding extension's Codecs. The link leads to the Extension Codecs page.

Clicking on each user extension in the Extensions table will open the extension specific **Extension Settings** menu. When Call Park service is enabled on the extension, it is displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible.

Add opens the **Add Entry** page where the type and the number of new extension should be defined. Page consists of the following components:

Extension text field is used to enter a new extension number. The extension number is a two-digit number. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" occurs. If the extension length is shorter than 2 digits, the error "Incorrect Extensions length" will prevent the creation of the extension. If an extension with the same number already exists in the Extensions Management table, the error "Extension already exists" will appear.

Please Note: Extension number cannot start with digits 0, 8 or 9.

Type drop down list is used to select the type of the extension (user, attendant or pickup group) to be created (for details see below).

Fig. II-55: Extensions Management - Add Entry page

Edit opens the **Edit Entry** page where a newly created user or attendant extension settings might be adjusted. To operate with **Edit**, one or more record(s) have to be selected, otherwise an error will occur: "No records selected".

The **Edit Entry** page consists of two frames. In the left frame settings groups are listed. Clicking on the corresponding settings group, its configuration options will be displayed in the right frame.

Please Note: Pay attention to save changes before moving among settings groups.

1.   General Settings

This group requires extension's personal information and has the following components:

Display Name is an optional parameter used to recognize the caller. Usually the display name appears on the called party's phone display whenever a call is performed or a voice mail is sent.

Password requires a password for the new extension.

The extension password may only contain digits. If non-numeric symbols are entered an "Incorrect Password: no symbol characters allowed" error will prevent making the extension.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error will appear: "Incorrect Password confirm".

Attached Line lists all free lines to where an extension may be attached.

Fig. II-56: Extensions Management - Edit Entry – General Settings page

Allow Call Relay enables the current extension to be used to access the Call Relay service in the Quadro's Auto Attendant. It is recommended to define a proper and non-empty password when enabling this feature in order to protect the Call Relay service from an unauthenticated access.

Use for Call Park allows to use the extension for the Call Park Service. It is recommended to use virtual extensions for this service and to configure all available codecs, so parked call won't be lost in case if a caller, who picks up the parked call, doesn't support some specific codecs. When Call

Park service is enabled on the extension, it is displayed without link in the Extensions Management table and extension pages and additionally supplementary services configuration pages will not be accessible.

When **External Call Policy** checkbox is enabled, all incoming IP calls to the corresponding extension will be handled by the external Policy Server.

The **Percentage of System Memory** drop down list allows to select the space for the extension's voice mails and uploaded/recorded greetings and blocking messages. The maximum value in the drop down list is equal to the maximal available space for voice messages on Quadro. While editing an existing extension and decreasing the voice mailbox size, the system will check the present amount of voice mails in the mailbox of the extension. If the memory required for these voice mails exceeds the size entered, the system will suggest either to remove all voice messages from the extension's voice mailbox or to select a larger size so that the existing voice messages can be stored in the mailbox.

2. SIP Settings

This group is used to configure the extension's SIP registration settings and consists of the following components:

Registration User Name requires a user name for the extension registration on the SIP server. The registration user name needs to be unique on the SIP server and is being displayed on the called phone whenever performing an IP call.

Registration Password indicates the password for the extension registration on a SIP server.

Confirm Registration Password is used to confirm the password. If the entered password does not correspond to the one given in the **Registration Password** field, the error will appear: "The passwords do not match. Please try again".

Registration SIP Server indicates the host address of the SIP server. The field is not limited regarding symbol usage and length as it can be either an IP address, e.g., 192.168.0.26 or a host address, e.g., sip.epygi.com.

Fig. II-57: Extensions Management - Edit Entry – SIP Settings page

Registration SIP Port indicates the host port number to connect to the SIP server. The SIP server port may only contain digit values, otherwise the error message "SIP Server Port is incorrect" will be displayed when applying the extension settings. If the SIP server port is not specified, Quadro will access the SIP server through the default port 5060.

Registration on SIP Server enables the SIP server registration option. If the extension has already been registered at some SIP server, its IP address will be displayed in brackets.

3. Advanced SIP Settings

This group is used to configure advanced SIP settings (Outbound Proxy, Secondary SIP Server and Outbound Proxy for the Secondary SIP Server settings and to define other SIP server specific settings).

SIP Outbound proxy is such a SIP server, where all the SIP requests and other SIP messages are transferred. Some SIP servers use an outbound proxy server to escape restrictions of NAT, e.g., Free World Dialup service uses an Outbound Proxy server. If an Outbound proxy is specified for an extension, all SIP calls originating from that extension are made through that outbound proxy, i.e., all requests are sent to that outbound proxy, even those call by Speed Calling.

The Secondary SIP Server acts as an alternative SIP registration server when the primary SIP Registration Server is inaccessible. If the connection with the primary SIP server fails, Quadro will automatically start sending SIP messages to the Secondary SIP Server, and will switch back to the primary SIP server, as soon as its connection is reestablished.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested for some SIP servers only, for others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If no reply is received from the primary SIP server within this timeout, the Secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will be sent to it once again.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name), the port number of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

RTP Priority Level drop down list is used to select the priority (low, medium or high) of RTP packets sent from corresponding extension. RTP packets with higher priority will be preceded first in case of heavy traffic.

Fig. II-58: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Remote Settings

This group is used to configure **SIP Remote Extension** functionality which is an advanced telephony feature that allows Quadro users to remotely operate on Quadro when being away. User needs to register a hardware or software SIP phone on the Quadro, by defining the Quadro's global IP address and an appropriate Username/Password. Registered SIP Remote phone can fully act as a phone connected locally to Quadro, i.e. use Quadro's PBX features, place and receive calls, access voice mails, etc.

Enable checkbox activates the SIP Remote Extension's functionality.

Please Note: **SIP Remote Extension** functionality may be enabled only for active (attached to an onboard FXS or IP line) extensions. Identification parameters used by the remote SIP device for registration on the Quadro should be defined in the **Username** and **Password** text fields.

When **Enable RTP Proxy** checkbox is selected, incoming and outgoing RTP streams to and from the remote SIP phone will be routed through Quadro, otherwise, when checkbox is not selected, RTP packets will be moving directly between peers.

When **Use Only When Registered** checkbox is selected, incoming calls towards the corresponding extension on the Quadro will be forwarded to the remote SIP phone, only in case it is registered. Otherwise, when remote SIP phone is unregistered, incoming calls will be routed to the line extension is attached to. When this checkbox is not selected, all incoming calls will be routed to remote SIP phone regardless on its actual registration.

The **Symmetric RTP** checkbox should be selected when remote extension is located behind the symmetrical NAT.
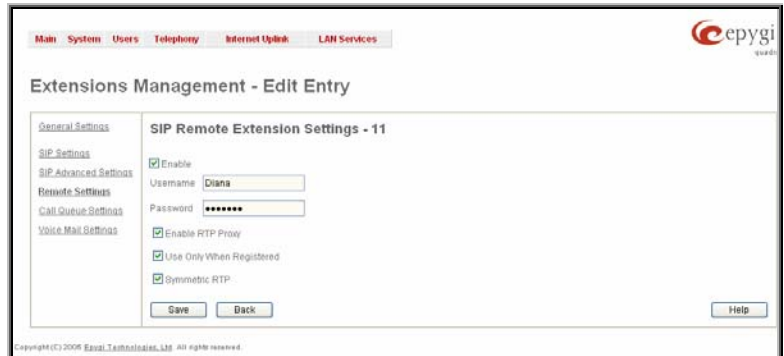
Fig. II-59: Extensions Management - Edit Entry – Remote Settings page

5. Call Queue Settings

This group is used to configure **Call Queue** service that allows to keep multiple incoming calls in the queue when being on the line and to answer calls in the order they have been received. Feature can be also used within Receptionist Management (see below for more details).

Enable checkbox activates the Call Queue functionality on the extension.

Call Queue Size text field requires the length of the call queue, i.e. the number of calls that can be held during extension being in call. If a maximal number of calls is already held in the call queue, next incoming call will be disconnected.

Max Call Queue Appearance text field requires the maximal number of active calls on the line, i.e. if 1 is configured in this field and extension is in call, next incoming call will go to the call queue. If 2 is configured in this field and extension is in call, next incoming call alert will be heard in the background (if Call Waiting service is enabled on the corresponding extension) and extension can hold the first call to answer the second one, either he can join the two calls into the call conference. However, the next incoming call will again go to the call queue.

Fig. II-60: Extensions Management - Edit Entry – Call Queue Settings page

Upload new call queue welcome message allows updating the active Call Queue welcome message (played when caller joins the extension's call queue), downloading it to the PC, or restoring the default one.

The **Remove call queue welcome message** functional link appears only when custom call queue welcome message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue welcome message** functional link appears only when custom call queue welcome message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Upload new call queue message allows updating the active call queue message (played upon caller being in the queue), downloading it to the PC, or restoring the default one.

The **Remove call queue message** functional link appears only when custom call queue message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue message** functional link appears only when custom call queue message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Browse buttons open the file chooser window to browse for a new Call Queue welcome message file. The uploaded files should to be in PCMU wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading if there is not enough memory available for the corresponding extension, which will cause the "You do not have enough space" warning.

6. Voice Mailbox Settings

This group is used to configure the voice mailbox storage and consists of a group of manipulation radio buttons used to define the location where voice mails will be collected.

- **Disable Voice Mail** – disables the Voice Mail service for the corresponding extension. With this selection, extension user will be unable to reach his Voice Mail Settings, but will be able to access his Voice Mailbox and manage with the existing voice mails.

- **Use Internal Voice Mail** – enables the Voice Mail service for the corresponding extension and defines the Quadro's internal storage as a location for the Voice Mails.

- **Use External Voice Mail** – enables the Voice Mail service for the corresponding extension and is used to define a remote Voice Mail Server as a location for the Voice Mails. With this selection, it is requires to enter the SIP URI of the Voice Mail Server where voice mails of the corresponding extension will be collected.

Fig. II-61: Extensions Management - Edit Entry – Voice Mailbox Settings page

Pickup Group & Access List

The **Pickup Group** service is used to monitor the calls addressed to a certain list of extensions and to pick up the calls ringing on the listed extensions. Service may be particularly used when a group of extensions are located in the same area, so the ringing on one of extensions can be heard by the persons sitting nearby. Feature allows to pick up the call ringing on the certain extension by dialing the number of the pickup extension.

Pickup Group list is used to define the extensions that can be monitored by calling the certain pickup extension.

Access List is used to define PBX, SIP or PSTN users that are allowed/forbidden to intercept the calls ringing on the extensions in the Pickup Group.

When user dials the pickup extension having several extensions of the pickup group ringing, the first (oldest in time) call will be picked up. When user dials the pickup extension having no ringing extensions of the pickup group, "No call is available to pickup" message will be played to the user. When user that is not listed in the **Access List** dials the pickup extension, password authorization (of the pickup extension) will be required to pick up the call. When a denied user dials the pickup extension, "Party does not accept your call" message will be played to the user.

For **Pickup Group** extensions, **Extensions Management** - **Edit Entry** page consists of **General Settings, SIP Settings** and **Advanced SIP Settings** pages. The **SIP Settings** and **Advanced SIP Settings** pages are the same as for the regular extensions and are described above, while **General Settings** page has a different content:

1. General Settings (for pickup group extension)
This group requires personal extension information and has the following components:

Display Name is an optional parameter used to recognize the caller. Usually the display name appears on the called party's phone display whenever a call is performed or a voice mail is sent.

Password requires a password for the new extension.

The extension password may only contain digits. If non-numeric symbols are entered an "Incorrect Password: no symbol characters allowed" error will prevent making the extension.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error will appear: "Incorrect Password confirm".

Fig. II-62: Extensions Management - Edit Entry – General Settings for pickup extension page

The **Edit Pickup Group** link leads to the page where a list of monitored extensions can be defined.

The **Pickup Group of Extension** page lists all extensions in the pickup group, i.e. those that can be monitored and the calls addressed to which may be picked up by calling the corresponding pickup extension.

Add functional button opens an **Add Entry** page with an only drop down list containing all available extensions on the Quadro.

Fig. II-63: Pickup Group of Extension page

The **Edit Access List** link leads to the page where users permissions to use the pickup service can be defined.

The **Access List of Extension** page lists all users (or a group of users, if wildcard is used) and the appropriate permissions to pickup the calls ringing on the extensions from the Pickup Group.

Fig. II-64: Access List of Extension page

Add functional button opens an **Add Entry** page where new user with corresponding permissions might be created. Page consists of the following components:

Call Type lists the available call types:

- PBX - local calls from Quadro's extensions
- SIP – calls through a SIP server
- PSTN – calls from global telephone network
- Auto – used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through Call Routing Table.

Address text field is used to define the address to be included in the Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If **PBX** call type is selected, the Quadro extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here.

Action drop down list is used to select the defined user's permissions (allow or deny) to use the pickup service for the extensions included in the Pickup Group.
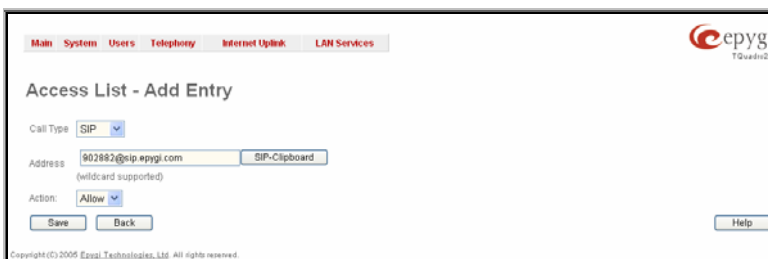
Fig. II-65: Access List of Extension –Add Entry page

For **Attendant** extensions, **Extensions Management** - **Edit Entry** page consists of **General Settings, Attendant Scenario**, **SIP Settings** and **Advanced SIP Settings** pages. The **SIP Settings** and **Advanced SIP Settings** pages are the same as for the regular extensions and are described above, while **General Settings** and **Attendant Scenario** pages' content is described below:

1. General Settings (for attendant extension)
This group requires personal extension information and has the following components:

Display Name is an optional parameter used to define the Auto Attendant's description. Usually the display name appears on the called party's phone display whenever a call is performed or a voice mail is sent.

With the **Enable FAX Forwarding** checkbox enabled, the system moves the incoming FAX to the selected extension if a FAX tone is detected on the Auto Attendant.

The **Extension to forward** drop down list is used to choose the extension where the incoming FAX addressed to the Quadro's Auto Attendant will be forwarded. The list contains only those extensions that have FAX support enabled. FAX support can be enabled from the Extension Codecs page.

Please Note: FAX forwarding is applicable only for incoming calls from PSTN and IP networks, it is not valid for PBX calls.
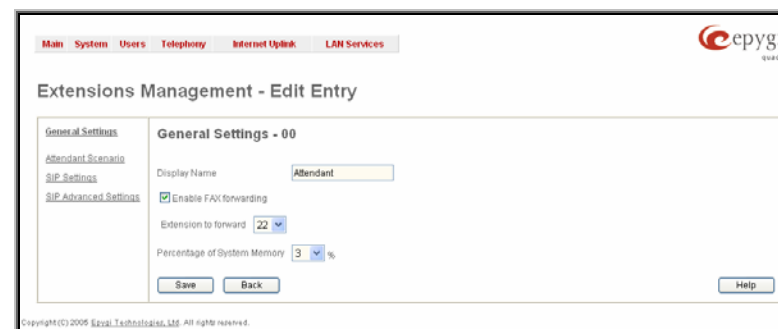
Fig. II-66: Extensions Management - Edit Entry – General Settings for Auto Attendant page

The **Percentage of System Memory** drop down list is used to defined the space for the Auto Attendant's system messages. The maximum value in the drop down list is equal to the maximal available space for voice messages on Quadro.

Fig. II-67: Extensions Management - Edit Entry – Attendant Scenario page

2. Attendant Scenario

This group is used to select between default and custom attendant functionality scenarios. When **Default** scenario is selected, a group of settings should be adjusted, user defined Auto Attendant welcome messages can be uploaded and the list of **Friendly Phones** can be configured. For **Custom** scenario, scenario script file (in EpygiXML coding, the coding standard can be found at Epygi Technical Support) should be defined and custom voice messages can be uploaded.

The **Default** manipulation radio button selection enables following components:

● **Send AA Digits to Routing Table** checkbox selection switches the Auto Attendant to the routing mode. Any inserted digits in the Connection menu will be parsed through the Routing Table on the Quadro.

> **Please Note:** This checkbox affects ONLY Connections Menu (see Auto Attendant Services). In Call Relay Menu, the routing prefix needs to be dialed (see Feature Codes) to parse the dialed number through the Routing Table.

● **Attendant Welcome Message -** this group allows updating the active Auto Attendant welcome message, downloading it to the PC, or restoring the default one. The group offers the following components:

The **Restore Default Welcome Message** checkbox allows restoring the Auto Attendant default welcome message file if another one has been previously selected. If the checkbox is selected, the file upload will be disabled.

Upload new welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading if there is not enough memory available for the corresponding extension, which will cause the "You do not have enough space" warning.

Browse opens the file chooser window to browse for a new welcome message file.

The **Download Welcome Message File** link appears only if a file has been previously uploaded. The link is used to download the audio file to the PC and opens the file chooser window where the saving location can be specified.

● **Routing Attendant Welcome Message -** this group is available for default 00 attendant only and allows updating a welcome message played when Auto Attendant acts in the routing mode (i.e., incoming calls to FXO line or ISDN timeslot are routed to the Routing agent), downloading it to the PC, or restoring the default one. The group offers the following components:

The **Restore Default Routing Welcome Message** checkbox allows restoring the routing Attendant welcome message file if another one has been previously selected. If the checkbox is selected, the file upload will be disabled.

Upload new Routing welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message. The system prevents uploading also if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning.

Browse opens the file chooser window to browse for a new routing welcome message file.

The **Download Routing Welcome Message File** link appears only if a routing welcome message has been previously uploaded. The link is used to download the audio file to the PC and opens the file chooser window where the saving location can be specified.

● **Friendly Phones -** the **Edit Authorized Phones Database** link refers to the Authorized Phones Database page where a list of trusted external phones can be created.

The **Custom** manipulation radio button selection allows to upload Attendant's custom scenario file and voice messages:

● **Upload Scenario File** indicates the file name used to upload a new scenario file. The uploaded file needs to be in EpygiXML format (the coding standard can be found at Epygi Technical Support) and is restricted to 20KB file size. **Browse** opens the file chooser window to browse for a custom scenario file.

● The **View/Download Scenario** link appears only when a custom scenario file has been previously uploaded and is used to view or download the scenario file. **Remove Scenario** link is used to remove a custom scenario file and to turn to default Auto Attendant scenario.

● **Upload Custom Voice Messages** link refers to the same named page where voice messages used in the uploaded custom scenario should be managed.

Fig. II-68: Upload Custom Voice Messages page

This page provides a possibility to upload voice messages to be played in the custom Auto Attendant scenario, as well as to remove and to download the uploaded files to PC.

Upload Custom Voice Messages page contains a table where uploaded custom voice messages are listed. Use **Download** functional button to download and **Remove** to delete the corresponding custom voice message. **Browse** opens a file chooser window to browse for a custom voice message.

The **Edit** functional button provides a possibility of editing multiple extensions at the time. In this case, fields that cannot be edited for multiple records have **Multiple** values in the **Edit Entry** page. When editing user and attendant extensions together, **Edit Entry** page displayed only those fields that are general for both user extension and attendant settings. Additionally, for the fields that need to be modified, a **Select to modify fields** checkbox alongside the corresponding field needs to be selected to submit changes, otherwise the fields will not be updated.

Delete removes the selected extensions. If no records are selected an error message occurs. Deleting an extension from the Extensions Table will automatically remove the Name attached to the deleted extension from the Extensions Directory.

Upload Universal Extension Recordings link leads to the page where universal default voice messages for all extensions are being defined.
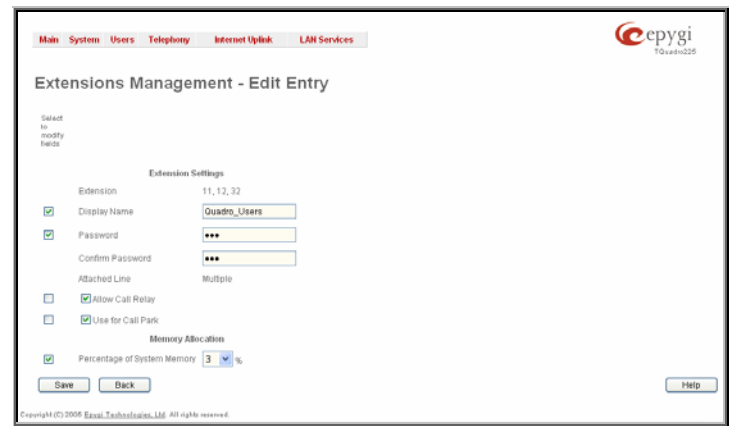
Fig. II-69: Extensions Management - Edit Entry page for multiple edit operation

To Configure an Extension

1. Press the **Add** button on the **Extensions Management** page. The **Add Entry** page will appear in the browser window.
2. Enter the desired extension number in the **Extension** text field and select the extension type from the **Type** drop down list.
3. Press **Save** to create a extension with the defined number.
4. Select the checkbox of the newly created extension in the **Extensions Management** table and press **Edit** button. The **Edit Entry** page will appear in the browser window.
5. Move through extension's configuration pages and fill the fields with desired information.
6. To apply extension settings, press **Save**.

To Delete an Extension

1. To remove an extension with all its settings select one or more checkboxes of the corresponding extensions that ought to be deleted from the **Extensions Management** table. Press **Select all** if all extensions ought to be deleted.
2. Click on the **Delete** button on the **Extensions Management** page.
3. Confirm the deletion with **Yes**. The extension will be deleted. To abort the deletion and keep the extension in the list, click **No**.

To Add an Authorized phone to the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. Press the **Add** button on the **Authorized Phones Database** page. The **Add Entry** page will appear in the browser window.
4. Choose the call type and enter a caller address in the corresponding text field.
5. Select a **Login Extension** and the **Automatically Enter Call Relay Menu** checkbox (if needed).
6. Enable **Call Back** service if needed and define a **Call Back Destination** in the same named field.
7. Fill in an optional **Description** in the appropriate field, if needed.
8. Press **Save** to submit the settings.

To Delete an Authorized phone from the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. To remove an authorized phone(s), select one or more checkboxes of the corresponding records that ought to be deleted from the **Authorized Phones Database** table. Press **Select all** if all records ought to be deleted.
4. Press the **Delete** button on the **Authorized Phones Database** page.

5. Confirm the deletion with **Yes** or cancel with **No**.

Extension Codecs

To establish IP voice communication, both partners have to use the same codec. During establishing the communication line, this codec is negotiated. If the caller does not find a fitting codec, the communication cannot take place. So, if you want to be reachable by preferably all IP calls, it is helpful to support as many codecs as possible. In this case, all the codecs that Quadro offers should be added to the **Active Codecs** table. On the other hand, some codecs require a high transfer rate - up to 64 kbit/s. If you are certain you do not want to use these codecs, you have to make sure they are not listed in the table **Active Codecs**.

The **Extension Codecs** page displays a list of **Active Codecs** and the state of the **Out of Band DTMF** and **FAX Support** features for Quadro extensions (also Auto Attendant).

Please Note: Use caution when configuring Auto Attendant Codecs as they are used by virtual extensions for redirecting the incoming calls.

The table **Active Codecs** lists active voice codecs for the selected line that are supported by Quadro. The order of records in the **Active Codecs** table is important for transmitting and receiving. A codec placed at the top of the table will be used as the preferred codec. If the remote party does not support the preferred codec, the following codecs will be tried out in a top-down order in the **Active Codecs** table.

Each record in the table has an assigned checkbox. It is used to select the record to be deleted or moved up or down.

An error occurs if no records are selected and the user activates the delete button: "No records selected". At least one codec must be attached to the line. When attempting to delete the last codec, this error will occur: "At least one codec should stay in the codec list".

Fig. II-70: Extension Codecs list

Add opens the **Add Entry** page where the user may add codecs supported by Quadro. The voice codec defines the voice compression algorithm for the incoming and outgoing DSP packages.

Codecs lists all codecs supported by Quadro. If no more codecs are available (all available codecs have already been transferred to the **Active Codecs** table), the **Add Entry** page will display the message "No Available Codecs" instead of the drop down menu.

Fig. II-71: Extension Codecs - Add Codec page

The **Move Up/Move Down** buttons are used to move the selected codec one level up/down in the table.

The **Out of Band DTMF Transport** checkbox enables DTMF code transmission in parallel with the voice stream. The destination receiving the DTMF code will play it locally if it supports the feature. This is helpful to avoid DTMF's loss upon bad traffic. This feature is valuable for all codecs but it is especially recommended to enable it in case low bit rate codecs (G729, G723, G726/16, etc.) are selected.

Enable T.38 FAX checkbox enables the FAX tone detection and the T.38 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line. **Enable Pass Through FAX** checkbox enables the FAX tone detection and the G711 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line.

If both of these checkboxes are enabled, T.38 codec will be used as preferred codec for FAX transmit/receive and if not acceptable by the peer, G711 codec will be used instead.

Please Note: If both of these checkboxes are disabled, no FAX transmission to the peer's voice mailbox will be possible. Checkboxes are applicable for FAX transmission/receipt over IP network only.

Enable Pass Through Modem checkbox enables the modem tone detection and the G711 codec support for the data transmission from/to the modem attached to the line. During data transmission, Silence Suppression (see RTP Settings) and Echo Cancellation are being disabled on the line.

Force Self Codecs Preference for Inbound Calls checkbox enables the usage of the own preferred codecs (if available on both peers) for the IP connection establishment on the extension.

Call Park Service

Call Park service is used to store a call on a specific number so that any other user on the system can retrieve it. For example, a user receives a call but wants to take it in a conference room where it is possible to speak privately. Transferring the call to the conference room is not an option, because the conference room it is transferred to might be in use, or the user is unable to walk to the conference room in time to answer the call. The user can use **Call Park** to place the call at a specific number and then retrieve the call on reaching the conference room.

To use the **Call Park** feature, the call parking service should be enabled for one or more extensions on the Quadro from the Extensions Management page.

To activate the Call Park service, the Quadro user should dial the appropriate digit combination (see Feature Codes) during the call. The destination party will be placed on hold, while the SIP username of the first available extension being configured for the call parking, will be played to the Quadro user. The Call Parking is valid for 15 minutes, during this time hold music (if configured) will be played to the parked destination party. When the **Call Park** timeout expires, the phone initiating call parking will start to ring, and if nobody picks up the parked call, or if the phone is off hook, the parked destination party will be disconnected automatically.

The pickup user will be able to pick up the parked call from any destination by simply calling the extension where the call has been parked. Either PBX or IP calls are allowed. For PBX calls, the extension number should be dialed; for IP calls, the - SIP address played by the Quadro when activating the **Call Park** service, if it is routed to the corresponding extension. The pickup user will be prompted to pass the authentication by inserting the password of the Quadro user (to which call has been parked) in order to retrieve the parked call.

Example: Call Park service is enabled for extension 23, which has been registered on the SIP Server under the 892220 registration username. Being in a call with user A, the Quadro user dials the appropriate calling code. As a reply, Quadro will play the 892220 to the Quadro user, while user A will go on hold. The Quadro user then moves to the different location and makes a SIP call to the 892220 number. When this SIP call is established to the 892220 number, user A will be then be connected to the Quadro user and the conversation will resume.

Please Note: Any PBX or IP calls addressed to the extension where the call has been parked, will require to pass the authentication to reconnect the Destination party being parked. The parked Destination party will be disconnected if an incorrect password has been inserted and authentication has been rejected. This is why, to avoid fortuitous calls receipt on the extension used for the call parking, it is recommended to use virtual extensions for the **Call Park** service.

Authorized Phones Database

Authorized Phones Database page is used to create a list of trusted external phones. If they are part of the Quadro Authorized Phones database, external SIP or PSTN users are free to access the Quadro Auto Attendant services without passing the authentication. When adding a friendly phone to the list, an existing extension has to be chosen whose parameters (extension number and password, as well as SIP and Speed Calling Settings) will be used automatically for the trusted caller access of the Quadro Auto Attendant. A direct connection to the **Call Relay** menu can be provided optionally.

The **Authorized Phones Database** page displays the **Authorized Phones Database** table where the trusted phones are listed. Only SIP and PSTN users can be added to the **Authorized Phones Database**.

The **Authorized Phones Database** table displays all trusted callers with their settings, e.g., call type, caller address, extension they automatically login with, information if they have automatic access to Auto Attendant (Call Relay Menu, etc.).

Fig. II-72: Authorized Phones Database

Each record in the table has an assigned checkbox. The checkbox is used to edit or delete the corresponding record. The "No records selected" error occurs if the user activates the edit or delete button having no records selected. The error "One record should be selected" appears if the user tries to edit more than one record. Each column heading in the table a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

The **Add** functional button refers to the **Authorized Phones Database- Add Entry** page where new trusted users may be entered.

The **Authorized Phones Database- Add Entry** page offers two group of input options:

Caller Settings

The **Call Type** drop down list includes possible incoming call types (PSTN, SIP or Auto). In **SIP**, the caller connects Quadro through a SIP server and **PSTN** means the caller is a PSTN user. **Auto** is used for undefined call types: destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

The **Caller Address** text field requires the caller's SIP address (see chapter Entering a SIP Addresses correctly) or PSTN number to be added to the trusted phones' list. The PSTN number length depends on the area code and phone number. The wildcard is supported in this field. If the caller address already exists in the **Authorized Phones Database**, the error

"The record already exists" appears when selecting the **Save** button.

The **Login Extension** drop down list provides all existing extensions on the Quadro. When calling the Quadro Auto Attendant, a trusted user will automatically login with the selected extension, i.e., extension number and its password will be automatically submitted by the Quadro system. The trusted user will directly access the Quadro Auto Attendant services. The SIP settings of login extension will be used while making IP calls.

The **Automatically Enter Call Relay Menu** checkbox enables direct access for the trusted user to the Quadro Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but still will be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

The **Automatically Enter Call Relay Menu** checkbox enables direct access for the trusted user to the Quadro Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but still will be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

The **Description** text field allows entering an optional comment.

Callback Settings

The **Enable Callback** checkbox selection gives a possibility for specified trusted caller to use the Instant Call Back service (see chapter Call Back Services).

The **Callback Destination** text field requires the destination PSTN number where Quadro should Instantly Call Back. If this field is empty, caller address will be implied as a callback destination.

Please Note: The Call Back service is functional and can be enabled only for PSTN callers and is valid for the PSTN callback destinations only.

Call Back Services

With the **Call Back** service the PSTN callers can save the call charge when calling to/through Quadro. Quadro gives a possibility to create a list of those trusted PSTN callers that are allowed to make free of charge calls to Quadro's Auto Attendant or through its Call Relay menu to the third party IP or PSTN destination.

Two types of Call Back are available on the Quadro: **Instant Call Back** and **Roaming Call Back**.

Instant Call Back

For **Instant Call Back** service a list of trusted PSTN callers must be pre-configured in the Authorized Phones Database on the Quadro. Call Back service should be enabled and a valid callback PSTN destination should be specified for the corresponding PSTN caller.

To use **Instant Call Back**, PSTN caller registered in the Authorized Phones Database should simply call to Quadro's PSTN number (that should be previously routed to the Auto Attendant or Routing Manager from the FXO Settings page) from the global PSTN network, let the call ring twice and then hang up. Call Back will get instantly activated, i.e. Quadro will call back to the defined Call Back destination and by answering the incoming call PSTN party will be automatically connected either to Auto Attendant or Routing Manager depending on the configuration of the corresponding FXO line on the Quadro.

Roaming Call Back

The **Roaming Call Back** allows to configure the call back by callers registered in Authorized Phones Database on the Quadro when calling from a PSTN number. **Roaming Call Back** is divided into two modes accessible from the Quadro's Auto Attendant: **Non Permanent Call Back** and **Permanent Call Back**.

Non Permanent Call Back can be used from the corresponding menu of the Quadro's Auto Attendant (see Call Codes). PSTN caller should pass the authorization by dialing existing extension number and an appropriate password. Normally, the PSTN caller's address should be detected automatically and then system will simply ask for the confirmation (in particular cases when caller is configuring Non Permanent Call Back service for him (or for anyone else) calling from the other number, other caller number should be defined here, so **Instant Call Back** will get activated only when calling from the defined caller number). If PSTN caller's address is not detected automatically, caller will be required to insert it manually (in this case Instant Call Back service will get activated immediately after hanging up). Call Back destination, where Quadro should call to, will be requested afterwards. It can be the same as the caller's address or can be different. When system accepts the call back settings, PSTN caller will be disconnected from the Quadro's Auto Attendant.

If the **Non Permanent Call Back** has been configured for the other caller address, system will wait till the incoming call will arrive from that other caller number, and after caller will let the call ring twice and hang up, Quadro will send a call to the defined PSTN destination in the next 45 seconds (if FXO line is available on the Quadro, network connectivity is fine and destination is reachable). Answering the incoming call, PSTN caller will be connected to the Quadro's Auto Attendant.

Next time, when PSTN caller reaches Quadro from the same number, he needs to pass the described procedure again since this was the one-time Call Back only and no entry was stored in the Authorized Phones Database on the Quadro.

Permanent Call Back service offers a convenience of registering new trusted PSTN Callers and to edit the Call Back destination of an existing PSTN Caller in the Authorized Phones Database. By calling Quadro's PSTN number (that is previously routed to the Auto Attendant) caller enters the Quadro's Auto Attendant and by **Permanent Call Back** menu (see Call Codes) he is able to register himself (or anyone else) as a trusted PSTN caller that is allowed to place free of charge calls to Quadro or through its Call Relay menu to the third party IP or PSTN destination as well as to modify the Call Back destination of an already registered Caller in the Authorized Phones Database.

Entering the **Permanent Call Back** menu, system will ask to login by dialing existing extension number and an appropriate password. PSTN caller's address confirmation will be required, or, if not detected automatically, it should be defined manually (in particular cases when caller is configuring Permanent Call Back service for him (or for anyone else) calling from the other number, other caller number should be defined here, so next time calling from that number, **Instant Call Back** will get automatically activated). Call Back destination, where Quadro should call to, will be requested afterwards. It can be the same as the caller's address or can be different. When system accepts the call back settings, the corresponding entry will be logged to the Authorized Phones Database.

PSTN caller will be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro in the next 45 seconds (if FXO line is available on the Quadro, network connectivity is fine and destination is reachable) if the detected PSTN caller address corresponds to the one applied by the caller (i.e. caller hasn't changed the detected caller address) or if caller address is not detected at all (due to system configuration problems or CO peculiarity). Otherwise, system will send a call back to the specified callback destination only if call arrives from the address logged in the Authorized Phones Database. Answering the incoming call, PSTN caller will be connected to the Quadro's Auto Attendant.

Being registered in the Authorized Phones Database once (by means of **Permanent Call Back** service or from the Quadro's Web Management), PSTN caller is able to use **Instant Call Back** service, i.e. next time when calling from the same PSTN number to the Quadro and hanging up after the second ring, the system will call the defined Call Back destination since the number is already registered in the Authorized Phones Database on the Quadro.

Upload Universal Extension Recordings

The **Upload Universal Extension Recordings** are to be defined by the Quadro administrator, will stand instead of the default voice messages for all extensions on the Quadro and will be used when no custom messages has been uploaded or recorded.

Following system messages can be uploaded from this page:

- **Hold Music** – played to the held user
- **Voice Mail Regular Greeting** – played when caller reaches the extension's voice mailbox
- **Voice Mail Out-of-Office Greeting** – played when caller reaches the extension's voice mailbox if Out-of-office greeting is enabled
- **Incoming call blocking** - played when a blocked user calls the extension
- **Outgoing call blocking** – played when extension dials a blocked destination

The **Upload Universal Extension Recordings** page consists of a table where universal voice messages are listed.

An **Upload** functional link is present for each not uploaded voice message in the table and is used to upload the custom system message. When a message is uploaded, **Upload** functional link is replaced by **Download** and **Remove** functional links respectively used to download to the PC and to remove the uploaded system message.

Memory Allocation group includes a drop down list used to specify the **Percentage of System Memory** for the universal extension recordings. The maximum value in the drop down list is equal to the maximal available space for voice messages on Quadro.
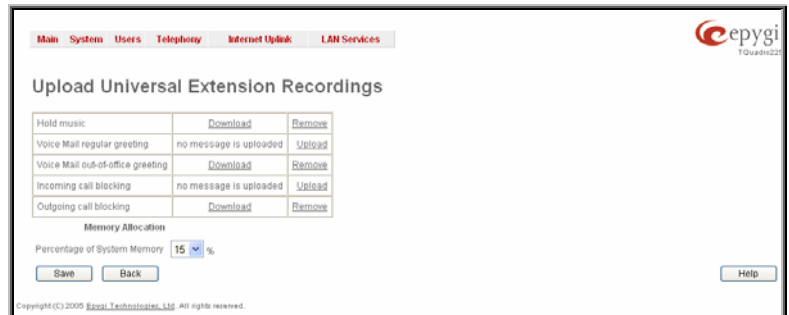
Fig. II-74: Upload Universal Extension Recordings page

Please Note: Changing the **Percentage of System Memory** on this page will stop any recordings of universal extension voice messages from the handset.

Receptionist Management

Receptionist feature on the Quadro offers a bunch of services to manipulate with multiple calls, to keep the calls in the queue with the perspective to be answered by the receptionist and finally to be forwarded to the corresponding destination, if needed.

Please Note: It is recommended to have the Snom360 IP phone for the receptionist in order to be able to use the services below.

Following services are available to the receptionist:

- Call Queue
- Extension Status
- Call Interception
- Voicemail Transfer
- Multi-Company Receptionist

Call Queue

Feature allows to keep multiple incoming calls in the queue when being on the line and to answer calls in the order they have been received. The usage of this service is not limited to receptionist only and can be used also by the extension user, if configured correspondingly.

The configuration of Call Queue feature is done from the Extensions Management – Edit Entry page, where the length of the call queue and the call queue appearance can be particularly defined. When Call Queue service is enabled, the second arriving call to the receptionist/extension user will be either set into the queue (if call queue appearance is 1) or will be ringing in the background of the active call (if call waiting is enabled for the user

and the call queue appearance value is greater than 1). If the call ringing in the background won't be answered, it will be transferred to the user's voice mailbox or, if no answer forwarding is enabled, will be forwarded to the corresponding destination.

If call is set into the queue, the caller will hear a message to wait until the call will be answered and a hold music. Once receptionist/extension user terminates the call, the next call in the queue will be ringing to the user.

Extension Status

Quadro provides a possibility to control and determine the actual state of the manager phones watched to the receptionist's IP phone (corresponding configuration should be done on the IP phone to watch a number of managers and set a programmable keys for them). Hence, the programmable key assigned to the corresponding manager will blink if incoming call is received and manager's phone is currently ringing, key lamp will be ON when manager is in call and will be OFF if manager's phone is in the idle state. Extension status can be used by the receptionist to get the actual information about the available managers for incoming call transfer.

Call Interception

The functionality of this service is limited to the capabilities of the Snom360 IP phone used as an official hardware for the Receptionist Management on the Quadro. To use the service of Call Interception, managers' phones watch option should be enabled on the IP phone and each manager should have a programmable key assigned on the receptionist's IP phone (please, refer to the IP Phone help to get information how to set up the programmable keys).

When incoming call addressed to the certain manager comes in, receptionist can see blinking of the corresponding programmable key and the caller's ID (for Snom360 only) on the phone's display. Receptionist is able to intercept the incoming call by pressing the blinking key. Caller will be connected to the receptionist then. If receptionist does not answer the call addressed to the manager, and if manager does not answer it either, call will be directed to the manager's voice mailbox, if enabled, otherwise disconnected.

Voicemail Transfer

Quadro allows receptionist to forward incoming calls directly to the voicemail of the attached extension. To do so, an appropriate routing pattern should be added to the Call Routing table. Hence, when transferring a call to the assigned extension, incoming call will directly go to the watched extension's voice mailbox.

Multi-Company Receptionist

Quadro provides a possibility to use the single IP phone (Snom 360) to manage the receptionist features for multiple companies at once. To do so, incoming line appearance on the phone should be created, attached to the IP line of the IP phone and be labeled to the corresponding company name. Being busy with a call related to one company, receptionist is able to receive also the calls related to other companies, calls will be ringing in the background, and receptionist can switch between the incoming calls. However, if receptionist does not answer the incoming calls, and if Call Queue service is enabled on the extensions, incoming calls will be stored into the queue specific for each company line.

Fig. II-75: Receptionist Management page

Receptionist Management page allows to configure IP phones to be used as a receptionist on the Quadro. Page contains the list of configured receptionists with information about the attached IP lines and watched extensions.

Add opens the **Receptionist Phone Configuration Wizard** where the new receptionist can be created and configured. Wizard consists of several pages.

The **Receptionist Phone Configuration Wizard - Page 1** has the following components:

Description text field requires the description of the receptionist to be configured.

Phone Model drop down list is used to select the IP phone model to be used by the receptionist. **Snom** selection in the list enables the MAC address text fields used to insert the **MAC Address** of the corresponding Snom IP phone.

Attached IP Lines text field requires the numbers of Quadro's IP lines used by the receptionist. IP lines should be separated by commas.

Fig. II-76: Receptionist Phone Configuration Wizard – Page 1

The **Receptionist Phone Configuration Wizard - Page 2** is available only for **Snom** selection in the **Phone Model** drop down list on the previous page. Page is used to set the correspondence between the selected IP lines and the available Programmable keys on the IP Phone.

To do so, select the IP lines corresponding to each programmable key from the drop down list on the page.

Fig. II-77: Receptionist Phone Configuration Wizard – Page 2

The **Receptionist Phone Configuration Wizard - Page 3** is available only for **Snom** selection in the **Phone Model** drop down list on the previous page. Page is used to set the watched extensions to the Programmable keys on the IP Phone.

To do so, select the extension from the corresponding drop down lists in order to associate the corresponding extension with the certain programmable key.

Please Note: A Programmable Key can be either assigned to an IP line or to a watched extension.

Fig. II-78: Receptionist Phone Configuration Wizard – Page 3

Please Note: Once a new receptionist is created, **Call Queue** feature will be automatically enabled with the corresponding **Call Queue Size** and **Max Call Queue Appearance** settings on all extensions attached to the IP lines defined in the **Attached IP Lines** text field.

Telephony Menu

Fig. II-79: Telephony Menu in Dynamo Theme

Fig. II-80: Telephony Menu in Plain Theme

Call Statistics

The **Call Statistics** page displays four tables and provides information on successful, unsuccessful and missed incoming and outgoing calls on the first three tables, and statistics settings on the fourth page. Call statistics allows the collecting of call events on the Quadro with their parameters and to search them by various criteria.

The **Statistics Settings** page offers the following input options:

The **Enable Call Reporting** checkbox enables Call Statistics reporting. The selected number of statistics entries will be displayed in the Call Statistics tables.

The **Maximal Number of Displayed Call Records** drop down lists are used to select the number of **Successful**, **Missed** and **Nonsuccessful** statistics entries to be displayed in the corresponding **Call Statistics** tables. If the record numbers exceed the numbers specified in these drop down lists, the oldest record will be removed.

The **Download Call Statistics** link is used to download all displayed statistics in a file that can be viewed with a simple text editor.

The **Clear all Records** button is used to clear all statistics records.

The **Number of Records** displays the current number of statistics entries in the table. For the successful calls, **Total Duration, Maximum Duration, Average Duration** and **Minimum Duration** statistics are displayed on top of the table.

The **Call Statistics: Successful Calls, Missed Calls and Nonsuccessful Calls** pages consist of the general information on successful, missed and unsuccessful calls, search fields and the calls table. The search components are as follows:

The **From** and **To** text fields are used to search by date and time. The data has to be entered in either of the following formats: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The time criteria is optional. **From** requires an earlier date and time than the **To** field. If the entered data does not meet this condition, the error message "Minimal date should be less than maximal date" prevents statistics filtering.

The **From** and **To** drop down lists are used to search by duration. The duration has to be selected from the list values. The **From** field has to indicate a shorter duration than the **To** field. If the inserted data does not meet this condition, the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.

Calling Phone and **Called Phone** respectively require the caller and called party's SIP address (see chapter Entering a SIP Addresses correctly), extension or PSTN number as search criteria. Wildcard symbols are allowed here.
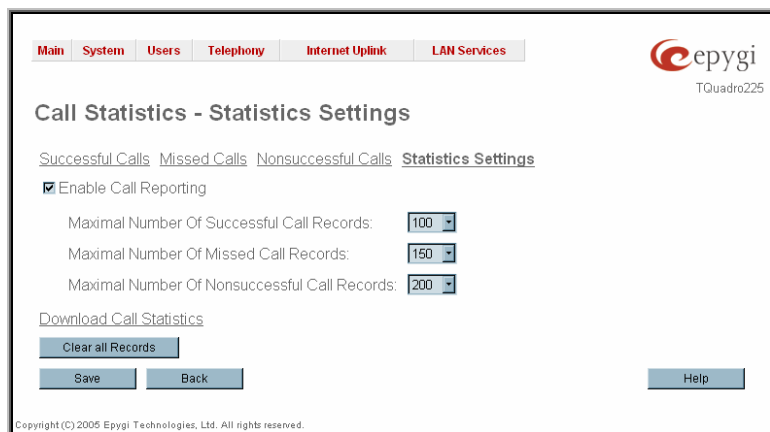
Fig. II-81: Call Statistics Settings page
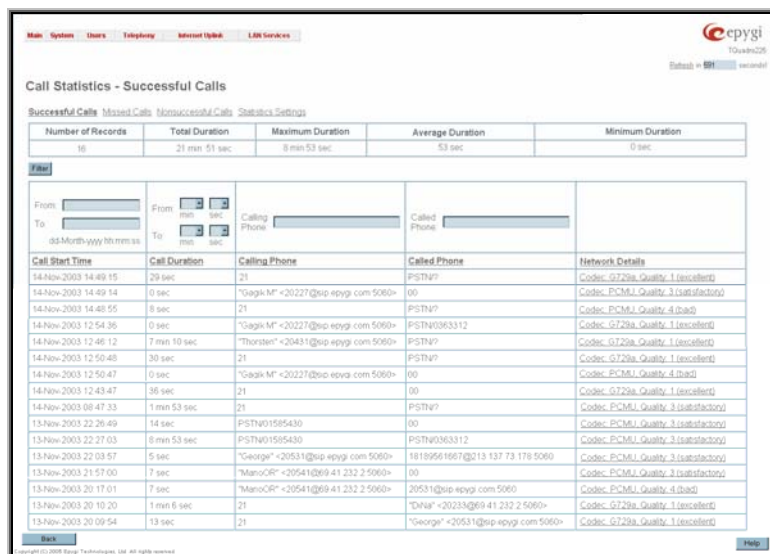
Fig. II-82: Call Statistics page

The **Call Statistics: Successful Calls, Missed Calls and NonSuccessful Calls** tables are lists of successful, missed and unsuccessful incoming and outgoing calls and their parameters (Call Start Time, Call Duration, Call destinations). Each column heading in the tables is a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

Network Details column is present in **Successful Calls** table only and provides brief information about the call quality and codecs used for receive and transmit packets. Clicking on the successful call details will open **RTP Statistics** page where detailed information about the established call is provided. **Call Detail** column is present in **Non Successful Calls** table only and indicates the reason of the call being unsuccessful.

Filter performs a search procedure by the selected criteria. The search may be done with several criteria at once.

To Enable/Disable the Statistics

1. Enter the **Call Statistics Settings** page.
2. Select/deselect the **Enable Call Reporting** checkbox to enable/disable statistics recording.
3. If enabling the statistics, the maximum number of records to be stored in the statistics table should be selected from the corresponding drop down lists.
4. Press **Save** to apply the new configuration.

To Filter the Statistics

1. Enter the desired criteria fields.
2. Press the **Filter** button to search the call reports within the **Call Statistics** table.
Please Note: To return to the complete **Statistics Table** clear all search criteria and press **Filter**.

To Reset the Statistics

1. Press the **Clear All Records** button in the **Call Statistics Settings** page.
2. Confirm the deletion with **Yes**. The call statistics will be deleted. To abort the deletion and keep the statistics information, click **No**.

RTP Statistics

The **RTP Statistics** page provides detailed information (Call Quality, Receive and Transmit Codecs, Number of Packets and Packet Sizes, Number of Received Lost Packets, Receive Jitter and Receive Maximum Delay) about the established call is provided.

Below is the legend for Call Quality definitions on the displayed RTP Statistics:

excellent - lost packets <= 1% & max_arrival_delay <= 100 ms
good - lost packets <= 5% & max_arrival_delay <= 200 ms
satisfactory - lost packets <= 10% & max_arrival_delay <= 400 ms
bad - lost packets <= 20% & max_arrival_delay <= 600 ms
very bad - lost packets > 20% or max_arrival_delay > 600 ms

Fig. II-83: RTP Statistics page

Please Note: RTP Statistics can be logged only when at least one of the call endpoints is located on the Quadro, e.g. it will not be logged when calls from an external user are routed to another external user through Quadro's routing rules, or when remote extension is used.

SIP Settings

The **SIP Settings** provide information on the SIP receive UDP and TCP ports and allows to select DNS server configuration for SIP and SIP timers scheme.

Fig. II-84: SIP Settings page

UDP Port indicates the SIP UDP (User Datagram Protocol) receive port number. By default 5060 is selected and used. The SIP UDP port cannot be in the selected RTP/RTCP port range for FXS and IP lines (see RTP Settings), otherwise the "Mapped port for SIP shouldn't be in RTP port range" error appears.

TCP Port indicates the SIP TCP (Transmission Control Protocol) receive port number. By default 5060 is selected and used.

Please Note: Quadro will not use TCP protocol as a transport for SIP messages if the **TCP Port** field is left empty.

Enable Session Timer enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.

The **DNS server for SIP** radio button group allows to choose between regular DNS servers configured in the DNS Settings page and specific DNS servers for the SIP traffic.

- **Use default** is used to apply regular DNS servers for the SIP traffic.
- **Specific** is used to enable SIP specific DNS servers. For this selection, both primary and secondary SIP DNS servers should be defined in the **SIP DNS 1** and **SIP DNS 2** text fields. At the least, a primary DNS server should be inserted.

The **SIP Timers** radio button group is used to define the timeouts of the SIP messages retransmission.

- **RFC 3261** will apply standard SIP timers described in the corresponding specification.
- **High availability** will apply SIP timers to shorten the call establishment, registration confirmation and registration failure procedures. This selection provides more firmness to the SIP connection but increases the network traffic on the Quadro.
- **Custom** allows defining manually the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session refresh timeout** SIP timers (in seconds).

RTP Settings

The **RTP Settings** page allows the administrator to configure the codec's packet size and silence suppression for each voice codec, to select the G726 codec standard, to define RTP/RTCP port ranges, etc. All parameters listed on this page may be modified and submitted.

The **Codec Properties** table lists all codecs with the corresponding packetization interval and information about silence suppression.

Edit opens the **Edit RTP Settings** page where the codec settings can be modified. To use **Edit**, only one codec may be selected at a time, otherwise an error occurs: "One record should be selected".

The **Packetization Interval** is the time interval between two RTP packets of the same stream. If the interval is increased, the overhead is decreased but the voice quality may deteriorate as a result. If the interval is decreased, the network load is increased and the delay is reduced.

Silence Suppression disables RTP packet transmission in case of no voice activity. This feature helps to avoid extra traffic if the RTP stream contains no voice. It is activated after two seconds of silence and restarted immediately if any audio appears.

The **G.726 Standard** radio buttons are used to select between packaging the G.726 codewords into octets. If you experience problems with G.726 voice quality having one of these packaging selected, try the other one.

- If **Use ITU_T specification** is selected, the ITU I.366.2 ("AAL2 type 2 service specific convergence sublayer for narrow-band services") type packaging of codewords is used, where packing code words into octets is starting from the most significant rather than the least significant digit in the octet.

- If **Use IETF RFC** is selected, the IETF RFC ("RTP Profile for Audio and Video Conferences with Minimal Control") type packaging of codewords is used, where packing code words is starting from the least significant position in the octet.

Fig. II-85: RTP Settings page

RTP/RTCP Port Range for FXS Lines and **RTP/RTCP Port Range for IP Lines:**

- **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.

- **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

As the specified maximum ports has to be higher than the minimum ports, the error message "Min port number should be less than max port number" will occur if this condition is not met. The port range may consist of digits only, otherwise the error "Incorrect Port Range: only Integer values allowed" occurs. The difference between Max and Min RTP ports should be 50 ports or less (according to the system's capabilities) otherwise the corresponding warning appears. RTP/RTCP Port ranges cannot include the defined SIP UDP ports (see SIP Settings) otherwise an error appears.

Telephone Event Draft Support enables telephony events transmission according to the draft-ietf-avt-rfc2833bis-04. The checkbox needs to be toggled if the SIP destination party phone or IVR has problems recognizing DTMFs generated by the Quadro.

Enable RTCP Support enables Real Time Control Protocol support and allows for the RTCP packets transmission. RTCP protocol is used for monitoring the RTP streams and changing RTP characteristics depending on Network conditions.

The **RTP Settings – Edit Entry** page offers a drop down list and a checkbox.

Packetization Interval contains possible values (in milliseconds) to be configured for the selected codec.

The **Enable Silence Suppression** checkbox selection enables voice activity detection for the selected codec.

Fig. II-86: RTP Settings - Edit Entry

To Edit Codec Parameters

1. Select the codec from the **Codecs Table** that is to be edited.
2. Press the **Edit** button on the **RTP Settings** page. The **Edit Entry** page will appear in the browser window.
3. Change values in **Packetization Interval** and/or enable/disable **Silence Suppression**.
4. To save the codec settings press **Save**, or to keep the initial data click **Back**.

NAT Traversal Settings

The **NAT Traversal Settings** page is divided into separate pages used to configure General NAT settings, SIP NAT parameters, RTP and STUN parameters for NAT and a page where the NAT Exclusion table may be filled.

The **General Settings** page consists of a manipulation radio buttons group to select the mode of the NAT Traversal usage for the SIP traffic (any incoming and outgoing SIP messages from and to the Quadro will be routed through the NAT PC).

*   **Automatic** – with this selection, system will analize the Quadro's WAN IP address and if it is in the IP range specified for local networks (according to RFC), the SIP traffic will be parsed over NAT, otherwise, if Quadro's WAN IP address is outside the specified IP range, no SIP traffic will be routed through NAT server.

*   **Force** – with this selection, all SIP traffic will be routed through NAT server.

*   **Disable** – with this selection, no SIP traffic will be routed through NAT server.

Fig. II-87: General NAT traversal page

The **SIP Parameters** page is used to configure NAT specific settings for SIP. and offers two independent group of settings:

UDP Parameters:
Manipulation radio buttons allow to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the SIP UDP traffic over NAT. STUN settings are configured on the STUN parameters page (see below).

Selecting **Use Manual NAT Traversal** allows to define manually the mapped settings for the SIP UDP traffic over NAT:

Mapped Host requires the IP address of the mapped host for SIP UDP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP UDP traffic over NAT.

TCP Parameters:

Mapped Host requires the IP address of the mapped host for SIP TCP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP TCP traffic over NAT.

Fig. II-88: SIP Parameters page

The **RTP Parameters** page is used to choose between the STUN and Manual NAT traversal connection for the RTP traffic and to define the RTP/RTCP ports for the connection over NAT.

Manipulation radio buttons allow to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the RTP UDP traffic over NAT. STUN settings are configured on the STUN Parameters page (see below).

Selecting **Use Manual NAT Traversal** allows to define manually the RTP/RTCP port ranges for the RTP traffic over NAT:

- The **Mapped Host** text fields require the Mapped Host for RTP traffic over NAT.

- **Mapped RTP/RTCP Port Range for FXS Lines** and **Mapped RTP/RTCP Port Range for IP Lines:**

  - **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.

  - **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

Please Note: RTP/RTCP Mapped Port ranges should be greater than or equal to the RTP/RTCP port ranges defined on the RTP Settings page.

Fig. II-89: RTP Parameters page

The **STUN Parameters** page enables automatic NAT configuration through the STUN server and is used to configure the STUN (Simple Traversal of UDP over NAT) client on the Quadro. The page requires the following data to be inserted:

The **STUN Server** text field requires the STUN server's hostname or IP address. The **STUN Port** text field requires the STUN server port number.

The **Secondary STUN Server** and **Secondary STUN Port** text fields respectively require the parameters of the secondary STUN server.

The **Polling Interval** drop down list contains the possible time intervals between referrals to the STUN server.

The **Keep-alive interval** text field gives the possibility to select the time interval (in seconds) for keeping NAT mapping alive.

The **NAT IP checking interval** text field indicates interval (in seconds) between the NAT IP checking attempts (used to distinguish the possible NAT IP address changes and to perform registration on the new host). Value should be in a range from 10 to 3600.

Fig. II-90: STUN Parameters page

The **NAT Exclusion Table** page includes a table where all possible IP ranges are listed that allows to exclude some network addresses from being NATed. For example, if a Quadro user needs to make SIP calls within the local network as well as outside of that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table. Otherwise, a malfunction may occur in SIP operations.

The **NAT Exclusion Table** page offers the following input options:

Each record in the table has its checkbox assigned to its row. This checkbox is used to delete or to edit the corresponding record. As only one record may be edited at a time, an error message appears, if none or more than one is selected.

Each column heading in the table is a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

The **Add Entry** page includes the following text fields:

Add opens the **Add Entry** page where a new IP range can be added.

Fig. II-91: NAT Exclusion Table page

Edit opens the **Edit Entry** page where the IP range can be modified. The page includes the same components as the **Add Entry** page.

The **NAT Exclusion Table** lists all possible IP ranges that are not included into the NAT process, but may be accessed directly. IP addresses that are not listed in the **NAT Exclusion Table** are accessed over NAT.

IP address requires the IP address that is placed behind NAT within the local network.

Subnet Mask requires the subnet mask corresponding to the specified IP address.

Fig. II-92: NAT Exclusion Table - Add Entry page

To Configure the NAT Exclusion Table

1. Press the **Add** button on the **NAT Exclusion Table** page. The **Add Entry** page will appear in the browser window.
2. Specify an **IP Address** and its **Subnet Mask** in the corresponding text fields.
3. Press **Save** on the **Add Entry** page to add the selected IP range to the **NAT Exclusion Table** list.

To Delete an IP Range from the NAT Exclusion Table

1. Select the checkboxes of the corresponding IP range(s) that ought to be deleted from the **NAT Exclusion Table**. Press **Select all** if all IP ranges ought to be deleted.
2. Press the **Delete** button on the **NAT Exclusion Table** page.
3. Confirm the deletion with **Yes**. The IP range will be deleted. To abort the deletion and keep the IP range in the list, press **No**.

Line Settings

The **Line Settings** are used to configure Quadro FXS and IP Line (if available on the board) settings. The **Line Settings** page consists of two pages: **Onboard Line Settings** page for onboard FXS lines configuration and **IP Line Settings** for IP Lines configuration.

Onboard Line Settings

The **Onboard Line Settings** page is used to configure Quadro lines and to define the caller ID detection type, configure remote party disconnect indication and select the ringer type on each of them. Additionally this page provides a possibility to enable Loopback diagnostics on the lines.

The page **Onboard Line Settings** shows the table **Available Lines** where all active lines of Quadro are listed with their **Attached Extension** (if attached, else none). Further, the table provides information about the selected **Ringer Type** and **Caller ID** detection method that is configured for the selected line. The caller ID detection method is different for various types of phones and can be found in the phone manual.

The **Loopback Settings** link takes you to the page where lines can be configured for loopback diagnostics purposes.

Fig. II-93: Line Settings Page

When pressing on the line number under the **Available Lines** column, the **Onboard Line Settings** page specific for the current line is opened and offers the following input options:

Caller ID drop down list contains various standards of Caller ID transmission used to send the calling party's information to the phone attached to the selected line:

- No Caller ID.
- FSK, send prior to the first ring.
- FSK, send between the first and second ring.
- FSK, send both prior to ring and between the first and second ring.
- DTMF, send prior to the first ring.
- DTMF, send between the first and the second ring.
- Combined, send both DTMF prior to the first ring and FSK between the first and the second rings.

The Quadro sends the current time/date to the called phone together with the caller's information.

Fig. II-94: Line Codec and Caller ID Settings page

A group of **Remote Party Disconnect Indication** parameters are used especially to configure the private PBX attached to the Quadro FXS port.

- The **Enable Busy Tone Indication** checkbox enables the busy tone transmission to the FXS port when the remote party being in call is disconnected. The **Busy Tone Duration** drop down list is used to select the period (in seconds) when a busy tone will be transmitted to the FXS port.

- The **Enable Power Disconnect Indication** checkbox enables the power cycling on the FXS line when the remote party being in call is disconnected. Power Disconnect is applied after the busy tone transmission on the FXS line. The **Disconnect Duration** drop down list is used to select the period (in milliseconds) when the FXS line power will be down.

The **Ringer Type** drop down list allows to select the frequency of the ringer supported by the phone attached to the line. Information can be found on the phone enclosure or in the phone's manual. Problems with the ringer might occur if the ringer type selected here does not correspond to the one supported by the phone.

Please Note: The supported ringer type can be found on the phone bottom, in the "**Ren:x.xN**" value where **N** is the ringer type supported by the phone, (e.g., if N=A, the TypeA ringer type should be selected, if N=B, the TypeB&Z ringer type should be selected).

The **Enable off-hook Caller ID** checkbox enables Caller ID transmission to the phone in the off-hook state attached to the certain line. Service is applicable to the phones supporting the Call Waiting Caller ID feature.

Information on the Caller ID system:

Caller ID is a service identifying the caller (when performing a call or sending a voice mail) and notifying the called party about the identity of the caller. Caller ID service is available only for phones with a display to show that information. Two types of Caller ID notification are available on Quadro: FSK and DTMF.

FSK Standard

The FSK standard supports caller ID indication either with the phone handset on-hook or if the called party is already busy with another call or operation (handset is off-hook). For internal calls, caller ID notification in FSK can show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's extension number. The second line shows the caller's nickname (if indicated in the configuration). For external IP calls, caller ID notification in FSK can also show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's user name. The second line shows the caller's nickname (if indicated in configuration). If the nickname is not available and there is a display name, provided by the caller party, the second line will display it, otherwise the URL in the format: username@host will be shown instead. For calls from the PSTN network, the entire caller ID message will be shown, sent by the PSTN station.

DTMF Standard

The DTMF standard supports caller ID indication only if the phone handset is on-hook (phone is free and ready to accept calls). This standard also has caller ID notification conditions but they are nonconfigurable as well. Caller ID notification in DTMF can show only one line of identifiable parameter on the called phone's display. For internal calls, it is the caller's extension number. For external IP calls, it is the caller's user name. For calls from the PSTN network, caller ID will display the caller's phone number only.

Please Note: DTMF supports only parameters consisting of digits. If any letter symbol has been used in the external caller user name, DTMF will display no caller ID at all.

To Configure the Line Settings

1. Select the line number that ought to be configured from the **Active Lines** column on the **Lines** table on the **Line Settings** page
2. Press on the line number link from the **Line Settings** table. The **Line Settings - Line#** page will appear in the browser window.
3. Use the **Caller ID** drop down list to select the caller ID detection system mode corresponding to the phone type.
4. Enable **Dialing Prefix With Caller ID** checkbox if needed.
5. Configure **Remote Party Disconnect Indication** parameters by selecting the corresponding checkboxes.
6. Define a **Ringer Type** from the corresponding drop down list.
7. Enable **Off-hook Caller ID** if needed.
8. Press the **Save** button on the **Line Settings - Line#** page to save the caller ID system and other line specific configuration settings.

IP Line Settings

The **IP Line Settings** page is used to configure IP lines for IP phones to be connected to the Quadro. Quadro provides the possibility to connect MGCP and SIP phones to its LAN side, assign the corresponding IP line to some active extension, and use MGCP and SIP phone as a simple phone with all telephony services of the Quadro, for example, call hold, waiting, transfer, etc. 2 IP Lines are available on the Quadro2x.

The **IP Lines Settings** page displays a table with the available IP lines on the Quadro. More IP lines can be enabled by entering the feature key in the Features page.

The **IP Lines** table lists all available IP lines with additional information about each of them: number of the extension attached to it, information about the phone type and the configuration details.

Each column heading in the tables is link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

Pressing on the **IP line** link in the **Available IP Lines** column, the **Edit IP Line** page specific for the current IP line is opened and offers a group of manipulation radio buttons that allows to enable the IP line and to configure it to for use by the SIP or MGCP phones:

Inactive - selection disables the corresponding IP line.

MGCP Phone - selection configures the IP line for an MGCP phone to be connected to the Quadro's LAN.

- The MGCP phone's **IP Address, Gateway Name** (optional) and the **Endpoint Name** will be required for this selection. Endpoint Name is defined on the MGCP phone and should match on Quadro for the successful connection between the MGCP device and the Quadro.

SIP Phone - selection configures the IP line for a SIP phone to be connected to the Quadro's LAN.

- **Phone Model** drop down list is used to select the IP phone model to be used by the receptionist. The selection other than **Other** enables the MAC address text fields used to insert the **MAC Address** of the corresponding SIP phone.

- **Line Appearance** text field requires number of simultaneous calls supported by the SIP phone.

- **Username** and **Password** are required for this selection, which should match on both the Quadro and the SIP Phone for successful connection establishment.

Fig. II-95: IP Line Settings page
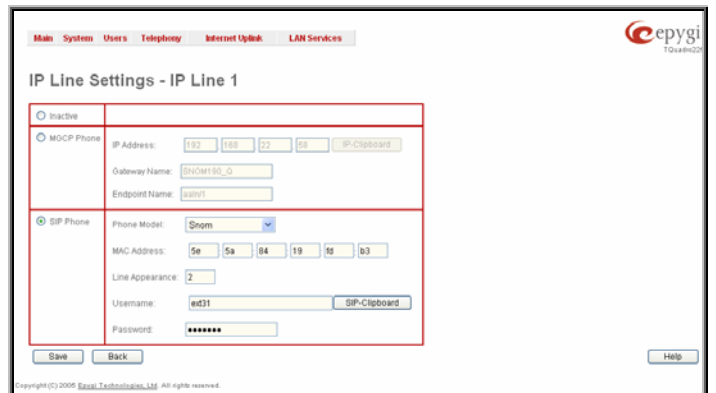
Fig. II-96: IP Line Edit page

Supported SIP Phones

Below is the list of SIP phones that can be automatically configured to work with Quadro2x:
- Snom 190, Snom 200, Snom 220, Snom 320, and Snom 360
- Polycom Soundpoint IP 300SIP
- Cisco IP Phone 7960
- Swissvoice IP 10S
- IP Dialog SIP Tone II (ST201)
- Aastra 480i
- Sipura SPA-841 IP

Loopback Settings

The **FXS Lines Loopback Settings** page is used to configure the lines for voice loopback diagnostics. When loopback is enabled on the line, any incoming calls to the corresponding line will be automatically picked up on the first ring and any voice towards the line will be automatically sent back to the caller, i.e., caller will hear themselves in the handset. **Loopback Timeout** gives a possibility to limit the voice loopback diagnostics duration, i.e., caller will be disconnected from the Quadro when the **Loopback Timeout** expires.

The **FXS Lines Loopback Settings** page shows the only table where all FXS lines of the Quadro are listed. Here, loopback diagnostics may be enabled/disabled and the Loopback Timeout can be adjusted for FXS lines.

The **FXS Lines Loopback** table lists all the FXS lines on the Quadro along with their loopback parameters (**Loopback State** and **Loopback Timeou**t).

The **Edit** functional link leads to the **FXS Lines Loopback Settings - Edit Entry** page where **Loopback Timeout** (in seconds) may be configured for one or more selected FXS line(s).

The **Enable/Disable Loopback** functional link is used to enable/disable the Loopback service on the selected FXS line(s).

Fig. II-97: IP Line Settings –Loopback page

FXO Settings

The **FXO Settings** are used to configure the FXO support that allows Quadro to connect to other PBXs or analog telephone lines. The **FXO Settings** also give a possibility to limit incoming or outgoing calls for the selected FXO line if required. Depending on the Quadro model, several FXO ports will be available on the board, thus giving the possibility to connect several PSTN lines to the Quadro and to use them simultaneously.

The administrator may assign a default recipient for each FXO line, where calls from the Central Office (PSTN) will be routed to. The assigned recipients become the Quadro "default users". If the Quadro Auto Attendant has been selected as "default user", a caller from the PSTN needs to go through the attendant menu to reach the desired extension.

Following FXO settings are available to be configured:

The **Enable FXO** checkbox selection activates FXO support for the selected FXO line.

The **Allowed Call Type** is used to choose the allowed call directions for the corresponding FXO line. The administrator may choose between:

- **Enabling incoming calls** (prohibiting outgoing calls) for the selected FXO line.
- **Enabling outgoing calls** (prohibiting incoming calls) for the selected FXO line.
- **Enabling both incoming and outgoing calls** for the selected FXO line.

Fig. II-98: FXO Settings page

The **Route incoming FXO Call to** manipulation radio buttons group allows to define the destination where incoming calls addressed to the corresponding FXO line will be forward to.

- **Extension** – selection allows to choose the local PBX user or auto attendant extension to forward calls to. If inactive extension is chosen from this list, the voice mail system will answer the call addressed to the corresponding FXO line. If Auto Attendant extension is chosen, it will become the "default user" of corresponding FXO line on the Quadro.

- **Routing** – selection allows to forward the incoming calls to the destination defined through <u>Call Routing</u>. Selection requires to enter a routing pattern to the corresponding field. Based on the registered PSTN users, caller will be able to reach the destination according to configuration in Call Routing Table.
  By choosing a destination, the Quadro administrator virtually assigns a default number that will start ringing whenever a call is initiated to the Quadro's PSTN number.

PSTN Number text field allows entering the PSTN number current FXO line is attached to. Field value is optional, used as an identification parameter for FXO lines and can be empty.

Alternative AC Termination Mode appears if the local country (Germany, Israel, France, etc.) selected for Quadro has two kinds of COs that use different types of AC termination. Contact your CO to learn about your AC termination mode. Selecting the checkbox may help if the voice quality over FXO is poor or echo is noticed.

ISDN Settings

Integrated Services Digital Network (ISDN) is distinguished by digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. The ISDN Basic Rate Interface (BRI) service offers two B channels (voice transfer) and one D channel (signaling data transfer). The BRI B-channel service operates at 64 kbit/s and is meant to carry user data; the BRI D-channel service operates at 16 kbit/s and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances.

ISDN service allows Quadro act as a user or as network. If connected to a private PBX, the Quadro should be configured in the network mode. If an ISDN trunk from the CO (Central Office) is connected to the Quadro, it should be configured as a user. Quadro supports MSN (Multiple Subscriber Number) service, i.e., it can be subscribed to multiple numbers from the CO, and two simultaneous calls can take place at a time.

The **ISDN Trunk Settings** page is used to configure the ISDN trunk and its signaling. The page offers the following input options:

The **Trunk Settings** table lists the available ISDN trunks on the Quadro and their settings (trunk name and interface types).

Edit functional button opens an **Edit Entry** page where ISDN Trunk specific settings can be configured (see below).

Start and **Stop** functional links are used to start/shutdown the selected ISDN trunk(s). When an ISDN trunk is in a shutdown state, no ISDN calls can be placed and received.

Restart functional link is used to bring channel(s) to the initial idle state on the both sides. When applying one of these options, any active traffic on the channel(s) will be terminated.

Copy to Trunk(s) functional link displays a page used to choose a trunk to which selected trunk's settings should be copied to.

Settings functional link leads to the **ISDN wizard** where ISDN signaling settings can be configured (see below).

Restore Default Settings functional link restores the default signaling settings of the selected ISDN trunk(s).

Edit Entry page consists of the following components:

Interface Type drop down list allows to choose between the **user** and **network** ISDN trunk interface configuration.

Coding Type drop down list allows to select between **a-law** and **mu-law** coding types.

LoopBackMode the loopback mode may be selected for trunk diagnostics purposes. When loopback is selected from this list, B1 and B2 channels will be switched to the loopback mode, D channels will stay operating normally and any incoming traffic towards the corresponding B1/B2 channels of the ISDN trunk will be automatically sent back to the traffic initiator.

Passive Mode checkbox is used to leave the ISDN Layer1 connection in Slave mode. When checkbox is selected, Layer1 remains idle when no calls are available, otherwise, when checkbox is not selected Quadro keeps its Layer1 always active.

ISDN Wizard consists of several pages.

The **ISDN Wizard - Page 1** has the following components:

Enable DDI Service checkbox enables the **DDI (Direct Dialing Inward) Service** on the trunk(s).

TEI Mode manipulation radio buttons are only available when DDI Service is disabled and are used to select the TEI selection mode:

- The **Automat** mode requires ISDN connection to be established on the first available channel. If **TEI Assignment on Power up** checkbox is selected Quadro tries to get TEI value after Power UP, otherwise Quadro tries to get TEI value on incoming or outgoing calls.

- The **Non Automat** mode enables the TEI Address text field that requires the channel number (digit values from 0 to 63) for connection establishment between the CO and the ISDN client. In this mode a private channel may be reserved for the connection and both call partners need to specify the same channel in their settings.
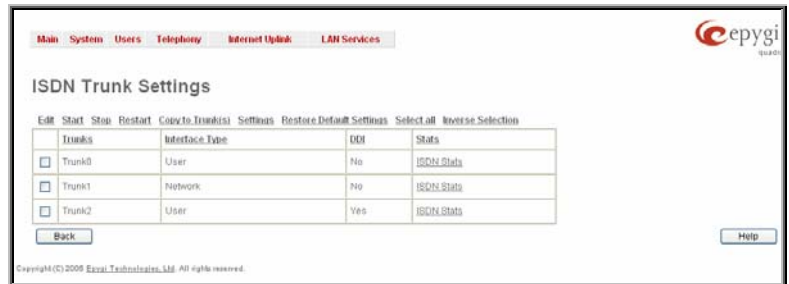
Fig. II-99: ISDN Settings page

Fig. II-100: ISDN Settings - Edit page
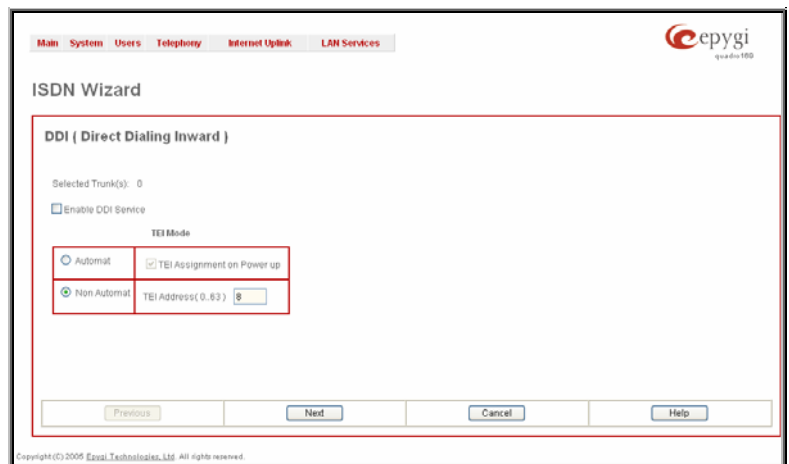
Fig. II-101: ISDN Wizard – Page 1

The **ISDN Wizard - Page 2** has the following components:

The manipulation radio buttons are present only for ISDN trunk acting in the user mode and when **DDI Service** is disabled from the previous page. Selection is used to choose whether other devices are connected to the ISDN bus or not and allows to switch the MSN (Multiple Subscriber Number) service. This service offers the possibility to have multiple ISDN numbers provided by the CO (Central Office) and is used to route incoming calls to the Quadro extensions, to the Auto Attendant or routing agent, depending on the subscribed number the call was received on.

Selecting **No other devices are connected to ISDN bus** disables the MSN service on the Quadro, and in this case all incoming calls will be routed to the selected destination.

The **Route Incoming call to** drop down list is present only when ISDN trunk acts in the user mode and contains the Attendant, a routing agent with two types of call routing possibilities, and also contains all the extensions of Quadro and allows for selecting the destination where the incoming calls ought to be routed to. Choosing the **Routing** selection will request the caller to pass the authentication (if enabled) and will invite them to dial the number that will be parsed through the Call Routing Table. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without any additional dialing.

Fig. II-102: ISDN Wizard – Page 2

Selecting **Other devices are connected to ISDN bus** selection enables the MSN service on the Quadro, and allows to configure the incoming MSN table. The **MSN Service** link leads to the **MSN Service** pages where MSN numbers can be created and modified.

Please Note: It is recommended to choose **Other devices are connected to ISDN bus**, if there are several subscribed numbers and multiple ISDN devices within the network.

The **MSN Service** page lists all existing MSN numbers on the Quadro and allows assigning MSNs to the Quadro extensions, to the Auto Attendant, or to the routing client with two kinds of call routing possibilities, where incoming calls will be routed.

Add functional button opens an **Add Entry** page where a new MSN number can be created. Field contains following components:

MSN Number text field requires the MSN number.

Fig. II-103: MSN Service page

Route Incoming Call to drop down list allows to select the destination where the incoming call to the certain MSN number will be routed to. Choosing the **Routing** selection will request the caller to pass the authentication (if enabled) and will invite them to dial the destination number to connect the user within the Quadro Network. Choosing the "**Routing with inbound destination number**" selection will automatically use the initially dialed number to connect the destination without any additional dialing.

Fig. II-104: MSN Service – Add Entry page

Selecting **Use Default outgoing MSN** allows to overwrite the source caller information with the one specified in the **Default outgoing MSN** text field when placing outgoing calls toward the CO. **Default outgoing MSN** text field requires the Quadro identification number that should be registered and recognized at the CO for outgoing calls. If this checkbox is enabled but no value is defined in **Default outgoing MSN**, empty caller information will be sent to the CO. If this checkbox is disabled, the source caller information will be forwarded to the CO.

The **ISDN Wizard - Page 3** has the following components:

Two groups of timers need to be provided. These settings are adjusted according to the Service Provider requirements.

ISDN L2 Timers:

- **Excessive Ack. Delay T200** configures the period in milliseconds (numeric values from 500 to 9999) between the transmitted signaling packet and its acknowledgement received.

- **Idle Timer T203** configures the period in milliseconds (numeric values from 1000 to 99999) for the ISDN client idle timeout.

ISDN L3 Timers:

- The **T302 Timer** text field requires the value for the T302 timer in milliseconds (digit values from 0 to 15000) and indicates the time frame system is waiting for digit to be dialed and when timer expires, it initiates the call.

- **T309 Timer** requires the value for the T309 timer in milliseconds (numeric values from 0 to 90000) responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is zero (0), the T309 timer will be disabled.

- **T310 Timer** requires the value for the T310 timer in milliseconds (numeric values from 1000 to 120000) responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) has not yet arrived.

- **Alert Guard Timeout** requires the value for the Alert Guard Timer in milliseconds (numeric values from 0 to 500) between CALL PROC and ALERT messages. Timer it is used when Quadro is connected to a slow ISDN-PBX. Recommended values are:
  - fast connection (0ms);
  - normal (150ms), default;
  - slow ISDN-PBX (350ms);
  - very slow ISDN-PBX (500ms).

Fig. II-105: ISDN Wizard – Page 3

Switch Type is another configuration parameter that depends on the Service Provider.

Channel Selection is used to select between the **Preferred** and **Exclusive** B channel selection methods. For **Preferred** channel selection, the CO answers to the call request by the first available timeslot, while for **Exclusive** channel selection, CO should feedback only by the timeslot used for the call request.

The **Bearer Establishment Procedure** drop down list allows selecting the session initiation method on the B channel. One of the following possibilities of the transmission path completion prior to receipt of a call acceptance indication can be selected:

- on channel negotiation at the destination interface
- on progress indication with in-band information
- on call acceptance

The **Calling Party Type of Number** drop down list allows to select the type identifying the origin of call.

The **Called Party Type of Number** drop down list allows to select the type identifying the subaddress of the called party of the call.

The **Called Party Numbering Plan** and **Calling Party Numbering Plan** drop down lists indicates correspondingly the numbering plan of the called party's and calling party's number.

Incoming Called Digits Size text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When field has 0 value, system uses either timeout defined in the T302 field or the **Sending Complete Information element** messages to establish a call. Independent on the value in this field, **Sending Complete Information element** and pound sign always cause the call establishment.

The **Generate Progress tone on IP** checkbox selection will generate the progress tone to IP (H.323 or SIP).

Enable CLIR Service checkbox selection enables Calling Line Identification Restriction (CLIR) service which displays the incoming caller ID only in case if Presentation Indication is allowed on the remote side. Otherwise, if CLIR service is disabled, caller ID will be unconditionally displayed.

When **Alternative Disconnection Mode** checkbox is not selected, Quadro will disconnect the call as soon as disconnect message has been received from the peer, otherwise, when checkbox is selected, Quadro's user may hear a busy tone when peer has been disconnected.

The **B1 Channel** and **B2 Channel** checkboxes enables/disables timeslots for voice transfer. Disabling the timeslot will prevent both incoming and outgoing calls.

Clicking on the **ISDN Stats** link will open the **ISDN Status** page that displays ISDN traffic statistics on the corresponding ISDN trunk. **ISDN Stats** link is displayed for every active trunk on the board and refers to the page where ISDN trunk and traffic statistics can be viewed.

The **ISDN Trunk Status** page provides information about the selected trunk state:

Link displays the ISDN link state: **up** or **down**.

Frame Synchronization displays the signal synchronization state in the trunk: **Yes** or **No**.

HDLC Receive shows the number of packets received in HDLC (High-level Data Link Control) format.

HDLC CRC Error shows the number of packets received with CRC (Cyclical Redundancy Check) errors.

HDLC Packet Abort displays the number of received aborted packets.

HDLC Transmit displays the number of packets transmitted in HDLC format.

HDLC Octet Count shows the number of error packets received in HDLC format.

SDN BRI Layer 2 statistics is displayed for received and transmitted packets:

TEI value shows the actual TEI value.

L2 State shows the actual BRI L2 state.

Information Frame shows the number of signaling packets for call initiation and termination.

Receive Ready displays the number of controlling packets while the ISDN link is up.

Receive Not Ready displays the number of controlling packets in case of inability to accept calls by destination.

SABME shows the number of packets upon connection establishment.

Disconnected Mode shows the number of packets when the connection is being disconnected.

Disconnect shows the number of packets upon connection termination.

Unnumbered Acknowledgement shows the number of packets upon accepting connection establishment/termination.

Framer shows the number of packets as a result of an error condition.

TEI Request shows the number of packets containing TEI (Terminal Endpoint Identifier) to initiate subscription of the device in the network.

Unnumbered Information Frame shows the number of broadcast signaling packets received for call initiation and termination.

Exchange Identification shows the number of received packets containing connection management settings.

Fig. II-106: ISDN Trunk Status page

ISDN BRI Layer 2 Errors statistics:

Incorrect Length shows the number of packets with an incorrect length.

Bad Supervisory Frame shows the number of packets with an incorrect supervisory header.

Bad Unnumbered Information Frame shows the number of packets with an incorrect unnumbered information frame header.

Bad Frame Type shows the number of packets with a bad frame type.

Bad Unnumbered Frame shows the number of packets with an incorrect unnumbered acknowledgement frame header.

Foreign TEI Value shows the number of packets with a bad or foreign TEI (Terminal Endpoint Identifier) value.

ISDN BRI Layer 3 statistics:

Active Calls shows the number of currently active calls in the selected trunk.

Outgoing Calls shows the number of all outgoing calls in the selected trunk.

Incoming Calls shows the number of all incoming calls in the selected trunk.

No ISDN trunk statistics are displayed on this page at first, but the page is automatically refreshed every 10 minutes. Statistics collected from that time as well as the last resetting of the counter will be displayed there. **System Uptime**, **Current System Time** and **Last Time Cleared** (last time ISDN statistics has been cleared) are displayed at the bottom of the page.

To reset the statistics counters press the **Clear** button.

Gain Control

The **Gain Control** settings are used to define the transmit and receive gains. For FXS lines, **Transmit Gain** defines the phone speaker volume and **Receive Gain** defines the phone microphone volume. For FXO lines/ISDN trunk **Transmit Gain** defines the level of voice transmitted from Quadro to the PSTN/ISDN network and **Receive Gain** defines the volume of voice received by Quadro from the PSTN/ISDN network.

The **Gain Control** page offers **Transmit Gain** and **Receive Gain** drop down lists for each line that contains allowed gain values, which can be set up by the administrator for every line.

Please Note: If the gain control has been configured incorrectly, DTMF digits may not be properly recognized. Gain control settings are strictly dependent on the location (country) of Quadro and the phone type. If a private PBX is attached to the FXO port on the Quadro, the voice level in the handset of the phone connected to the Quadro FXS port may be too loud (depending on the PBX type and configuration), which can be adjusted by decreasing the FXO **Receive Gain** to three or to zero.

The **Restore Default Gains** button restores the default values.

Fig. II-107: Gain Control page

Call Routing

The **Call Routing** service simplifies the calling procedure for Quadro users, i.e., any kind of calls (internal, SIP, PSTN or IP-PSTN) can be placed in the same way. No SIP registration is needed for extensions to make routing calls.

The **Call Routing** page offers the following components:

- The **Route all incoming SIP calls to Call Routing** checkbox that is used to route ALL incoming SIP calls (whether the pattern matches the extension's SIP registration username or not) to the Call Routing table. No digits will be stripped in this case.

- The **Call Routing Table** link leads to the **Call Routing** table where routing patterns may be defined manually.

- The **Local AAA Table** link leads to the page where local AAA (Authentication, Authorization, and Accounting) database can be managed.
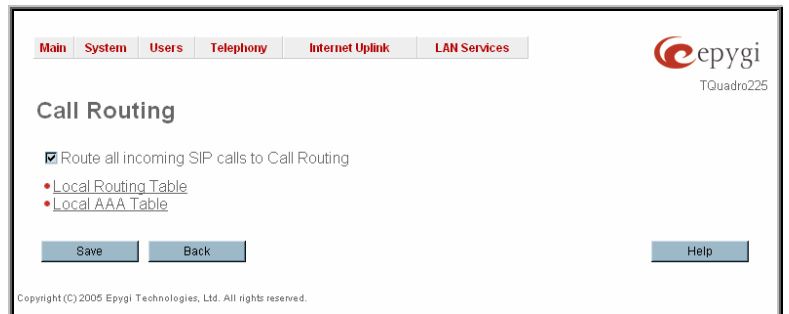
Fig. II-108: Call Routing page

Fig. II-109: Call Routing table

Defining patterns in the **Call Routing Table** avoids registering Quadro at the routing management server and gives a possibility to establish a direct connection to the destination or to use a SIP server for call routing.

The **Call Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and inbound caller settings, RTP Proxy and Date/Time period settings, metric and description), as well as automatically created and undeletable patters created from the System Configuration Wizard. The value **invalid** is displayed beside the ISDN routing pattern, if the ISDN trunk settings (ISDN interface type, signaling type, etc.) have been changed since defining the corresponding route. Invalid ISDN patterns will not be allowed.

If the route has an **Authentication** or an **Authentication&Accounting** selected from the **AAA Required** checkbox group, it will have a link to the **Users List** in the **Call Routing table**. **Users List** page contains a list of authorized users defined from the **Local AAA Table**, and gives a possibility to enable/disable authentication of each user for the particular route.

Since **Call Routing Table** may have multiple entries that could match to same pattern, the table will be internally rearranged according to the rules with these consequences:

- The pattern matching best to the Best Matching Algorithm will have the higher position in the rearranged list

- If multiple patterns equally match to the Best Matching Algorithm, the pattern with the lower metric will get the higher position in the rearranged list

- If the multiple patterns with the same metric have been matched to the Best Matching Algorithm, the pattern in the higher position in the table will get the higher position in the rearranged list.

The pattern in the highest position of the rearranged list will be considered as the preferred one. Second and subsequent matching patterns will be used, if the destination refused the call due to the configured Fail Reason.

The **Enable/Disable** functional buttons are used to enable/disable the selected route(s). Disabled routes will take no effect while enabled routes will be parsed when initiating routing calls. The **State** column in the **Call Routing Table** displays the current state of the routes (enabled/disabled).

Add starts the **Call Routing Wizard** where a new routing pattern may be defined. The **Call Routing Wizard** is divided into several pages: Page 1 displays the following components:

Pattern requires entering the routing pattern's identification. To make a specified call, the appropriate routing pattern should be dialed. Wildcards are allowed here (see chapter Entering a SIP Addresses correctly). '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers, '!' symbol is used for exclusion ("!5a" inserted in Pattern field means all patterns except those equal to 5a). For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified pattern; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified pattern.

Number of Discarded Symbols (NDS) requires the number of symbols that should be discarded from the beginning of the routing pattern. The field should be empty if no digits need to be discarded. Only numeric values are allowed for this field, otherwise an error message occurs: "Error: Number of Discarded Symbols is incorrect - digits allowed only".

Prefix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in front of the routing pattern instead of the discarded digits.

Suffix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in the end of the routing pattern. (For example, if the routing **Pattern** is 12345, the **Number of Discarded Symbols** is two, and the **Prefix** is 909 and **Suffix** is 0a, the final phone number will be 9093450a.)

Call Type gives a possibility to select the call type (PBX, PBX-Voicemail, FXO, SIP, IP-PSTN or ISDN). **PBX** call type is dedicated for call routing to the local PBX extension, and **PBX-Voicemail** call type is dedicated to route the calls directly to the voice mailbox of the local PBX extension.

Metric allows entering a rating for the selected route in a range from 0 to 20. If no value is inserted to this field, 10 will be taken as the default. If two route entries match a user's dial string, the route with the lower metric will be chosen.

The **Description** text field requires an optional description of the routing pattern.

The **Filter on Caller / Call Type / Modify Caller ID** checkbox selection allows limiting the functionality of the current route to be used by the defined caller(s) only. If this checkbox is enabled, inbound caller information (**Inbound Caller Pattern**, **Inbound Call Type, Inbound Port ID**, etc.) will be required later in the **Call Routing Wizard**.

The **Set Date / Time Period(s)** checkbox selection allows to define a validity period(s) for current routing pattern to take place and to define pattern date/time rules. When this checkbox is enabled, **Call Routing Wizard** - Page 5 will be displayed.

The second page of the **Call Routing Wizard** offers different components depending on the **Call Type** selected on the previous page.

Use Extension Settings is applicable to SIP and IP-PSTN call types only and allows to select the extension (also Auto Attendant) on behalf of the call that will be placed. The SIP settings of the selected extension will be used as the caller information. If no entry is selected in this list, the original caller information will be kept. When **Keep original DID** checkbox is selected, called destination will receive the original caller's information, rather than the information of extension selected from the **Use Extension Settings** list.

Destination Host requires the IP address or the host name of the destination (for a direct call) or the SIP server (for calls through the SIP server).

Destination Port requires the port number of the destination or of the SIP server.

User Name and **Password** require the identification settings for the public SIP server or servers requiring authentication.

The **Multiple Logons (ML)** checkbox is available only for the IP-PSTN call type and allows/denies multiple logon to the public SIP server with the same username at the same time.

Fig. II-110: Call Routing Wizard - page 1

Fig. II-111: Call Routing Wizard - page 2

Use RTP Proxy checkbox is available for SIP and IP-PSTN call types and is applicable only when route is used for calls through Quadro between peers both located outside the Quadro. When this checkbox is selected, RTP streams between external users will be routed through Quadro, otherwise, when checkbox is not selected, RTP packets will be moving directly between peers.

A group of **AAA Required** checkboxes is used to choose one or more Authentication, Authorization, and Accounting (AAA) settings:

- **Local Authentication** – with this checkbox selected, callers will need to pass authentication through Local AAA table (see below) when dialing the current pattern.

- **RADIUS Authentication and Authorization** – checkbox is present for all call types except PBX calls and when RADIUS client is enabled. With this checkbox selected, when dialing the current pattern, callers will need to pass the authentication through RADIUS server (see above).

- **RADIUS Accounting** - checkbox is present for all call types except PBX calls and when RADIUS client is enabled. With this checkbox selected, no authentication will take place, but a caller identifying CDR (call detail report) will be sent to the RADIUS server. Checkbox selection enables accounting on the RADIUS for the certain call.

If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.

The **Fail Reason** drop down list indicates available failure reasons and contains different failure reasons, depending on the call type selection on the previous page. Following Fail Reasons may be available in this list:

- **Cannot Establish Connection -** failure reason is available for FXO and ISDN calls only and indicates cases when connection cannot be established.

- **Wrong Number –** available for PBX, SIP and IP-PSTN call types and indicates cases when the dialed number is wrong.

- **Busy -** available for PBX, SIP and IP-PSTN call types and indicates cases when the dialed destination is busy.

- **Network Failure** - available for SIP and IP-PSTN call types and indicates cases when system overload, network failure or timeout expiration occurred.

- **Other -** available for SIP and IP-PSTN call types and indicates cases when authorization, negotiation, not supported or request rejected or other unknown errors occur.

- **System Failure -** available for SIP and IP-PSTN call types and indicates cases indicated in **Network Failure** and **Other** fail reasons.

- **None –** available for all call types and indicates no fail reason.

- **Any -** available for all call types and indicates any of above mentioned fail reason.

If the call cannot be established due to some of the selected Failure Reason, the call routing table will be parsed for the next matching pattern and, if found, the call will be routed to the specified destination.

SIP Privacy manipulation radio buttons group is available for SIP call type only and allows to select the security of the SIP route by means of hiding (or replacing, depending on the configuration of the SIP server) the key headers of the SIP messages used to establish the call.

- **Default Privacy –** with this selection, no Quadro specific SIP privacy will be applied, all privacy will be relied on the configuration of the SIP Server.

- **Disable Privacy –** with this selection, no SIP call security will be disabled, all headers of the SIP message will be transparently visible to the destination.

- **Enable Privacy -** with this selection, SIP privacy will be specified for the corresponding route. Selection enables a group of checkboxes to choose the key headers to be fully or partly hidden or replaced. **Require Privacy** checkbox selection is used to restrict the delivery of the SIP message if either of the selected headers cannot be hidden (or replaced, depending on the configuration of the SIP server) before being sent to the destination.

The **Port ID** drop down list is present for FXO and ISDN call types and contains FXO line numbers and ISDN trunks. **Any Local** and **Any@Any** selections are available for the FXO call type only and give a possibility to route calls via the first available local FXO line or any FXO lines (including shared on other Quadro boards) respectively.

The **Call Routing Wizard** - Page 3 appears if the **Fill Call Source Information** checkbox previously had been enabled on Page 1 of the **Call Routing Wizard**, and it will require information about the Inbound caller.

The **Inbound Caller Pattern** field requires the caller's address where the current route will be applied. Alphanumerics and any characters supported in the SIP username are allowed for this field. Wildcards are allowed here (see chapter Entering a SIP Addresses correctly). '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified pattern; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified pattern. The **Inbound Number of Discarded Symbols** and **Inbound Prefix** text fields are hidden only when an **FXO** call type has been selected from Page 1 of the **Call Routing Wizard**. The **Number of Discarded Symbols (NDS)** text field requires the number of digits that should be discarded from the beginning of the **Inbound Caller Pattern**. The field should be empty if no digits need to be discarded. Only numerics are allowed for this field, otherwise an error message occurs: "Error: Number of Discarded Symbols is incorrect - digits allowed only".

Fig. II-112: Call Routing Wizard - page 3

The **Inbound Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Inbound Caller Pattern** instead of the discarded digits. (For example, if the routing pattern is 12345, the Number of Discarded Symbols is two, and the prefix digits are 909, the final phone number will be 909345.) Wildcards are allowed here (see chapter Entering a SIP Addresses correctly).

The **Inbound Call Type** drop down list gives a possibility to select the call type (PBX, SIP, ISDN, FXO) used by the inbound caller to reach the Quadro.

The **Next** button will open a **Call Routing Wizard** - Page 4 where different information about Inbound Caller will be required depending on the selected **Inbound Call Type**. For the **SIP** Inbound Call Type, the **Inbound Host** text field will require one or more IP addresses or host names of SIP server where the caller is registered, or the caller's device in case of direct calls, separated by a space. If the **FXO** or **ISDN** Inbound Call Types are selected, the **Inbound Port ID** drop down list will require selecting the FXO line number or ISDN Trunk correspondingly, and on the next step, a list of timeslot(s) used to receive calls from the defined caller.

The **Call Routing Wizard** - Page 5 appears if the **Set Date / Time Period(s)** checkbox previously had been enabled on Page 1 of the **Local Vall Routing Wizard**, and it will require information about the pattern validity period(s).

Page provides selection between **Typical** and **Custom** date/time rule definition.

Typical selection contains a group of radio buttons that are used to select the frequency of the corresponding routing pattern to take place:

- **Daily**
- **Weekly** – the preferred weekday(s) should be selected for this option.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and month should be selected for this option.

In **Available Time Period** drop down lists, the time range of the pattern validation should be defined. Any time selected in this field will be considered corresponding to the Quadro's Time/Date Settings.

Custom selection provides a possibility to manually define the validity period(s). Use following format to insert pattern date/time rule(s):
[Month,Month-Month,...][Day-Day,Day,...][hh:mm-hh:mm,...]; ...

Fig. II-113: Call Routing Wizard - page 5

Please Note: Established patterns based on the **Emergency Codes and PSTN Access Codes Settings** in the System Configuration Wizard will be marked in bold and will be placed at the first position in the Call Routing Table. Additionally they cannot be modified and deleted from the Call Routing Table.

The **Duplicate** functional button is used to create a routing pattern with the settings of an exiting one. This is to avoid configuring a new routing entry completely by duplicating an existing entry with different settings. To use the **Duplicate** button only one record may be selected, otherwise an error will occur: "One row should be selected". The **Duplicate** button opens the **Call Routing Wizard** where all fields except the **Pattern** field are already filled in. **Pattern** for the new route will be required anyway.

The **Move Up/Move Down** buttons are used to move call routing patterns one level up or down within the **Call Routing** table. The consecution of the routing patterns is important when making routing calls as the **Call Routing** table is parsed from the top down and routing will take place according to the first pattern that matches the dialed number. The **Move To** button is used to move the selected entry to some other position in the Call Routing Table, which will increase or decrease the selected pattern's priority. Pressing the button will open the page where the row number should be specified, together with the position the selected entry is to be placed (before or after the defined row).

The **Local AAA Table** page allows to manage local authentication and authorization database. Callers dialing the routes which have an AAA (Authentication, Authorization, and Accounting) option enabled, will pass the authorization on **Local AAA Table** by phone number or username/password, depending on corresponding entry configuration on this page.

If the detected phone number of the caller dialing a route which has AAA option enabled, is registered in the **Local AAA Table**, caller passes authorization automatically. If the caller ID service is disabled or the caller's phone number is not registered, the caller is asked to enter registration user name and password.

The **Add** functional button opens the **Call Routing – Local AAA Table - Add Entry** page where new local AAA record can be created.

Fig. II-114: PSTN User Registration page

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the way of authorization and other parameters:

- **Authentication by Caller ID** – selection is used to set the authentication based on the caller's phone number (which is considered to be automatically detected). The **Phone Number** text field requires caller's phone number. Only numeric and wildcard characters (see chapter Entering a SIP Addresses correctly) are allowed for this field. '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number.

- **Authorization by Username and Password -** selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication user name. Only numeric values are allowed for this field, otherwise the "Incorrect Username - digits allowed only" error message occurs. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the "Incorrect Password - digits allowed only" error message occurs.

The **Expiration Date and Time** drop down lists are used to set the date and time when the registration is to expire.
The **Expires in** checkbox is used to enable the **Expiration Date and Time** feature.
The **Description** text field required an optional description about the calling party.

Fig. II-115: PSTN User Registration - Add Entry page

To make a Call Routing pattern

1. Click on the **Call Routing Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Call Type** from the drop down list.
6. Define the **Metric** or leave the default.
7. Enter a **Description** if needed.
8. Enable the **Filter on Caller / Call Type / Modify Caller ID** checkbox, if the route functionality should be limited depending on inbound caller information.
9. Enable **Set Date/Time Period(s)** checkbox, if route should be functional within certain time/date interval.
10. Press **Next**.
11. Select user or attendant extension from **Use Extension Settings** drop down on behalf of which the call will be placed.
12. Specify the **Destination Host** and **Port Number**, **Username** and **Password** if **IP** or **IP-PSTN** call type has been selected. For **IP-PSTN** call type, enable **Multiple Logons** if necessary. Enable **Use RTP Proxy** checkbox, if needed.
13. Choose the Authentication and Accounting method from **AAA Required** drop down list.
14. Choose a **Fail Reason** from the corresponding drop down list.
15. Press the **Next** button.
16. If **Filter on Caller / Call Type / Modify Caller ID** checkbox has been previously enabled and the call type is different from the FXO, fill **Inbound Caller Pattern** in the corresponding text field, choose the needed value from **Inbound Call Type** drop down list, as well as **Inbound Number of Discarded Symbols** and **Inbound Prefix** values.
17. Press the **Next** button.
18. If **IP** has been selected on the previous step in the **Inbound Call Type** drop down list, then **Inbound Host** should be inserted in the current page. If **FXO** or **ISDN** has been selected in the **Inbound Call Type** drop down list, then the ISDN trunk or the FXO line number should be selected here.
19. If **Set Date/Time Period(s)** checkbox has been selected on the first page, pressing **Next** will open **Date/Time Rules** page where route validity should be defined.
20. Press the **Finish** button to establish a local route with the inserted settings.

To create a local AAA entry

1. Click on the **Local AAA Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Local AAA Table** page.
3. Choose the Authentication type.
4. Enter the **Phone Number** or the **Username** and **Password** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

Best Matching Algorithm

The **Best Matching Algorithm** is used by the Routing Agent (RA) to sort the list of the patterns that match a dialed number. Sorting is done by the following principle: **the more the pattern matches the dialed number, the higher its priority.**

To decide which of the selected patterns matches the dialed number more in comparison with the others, the following list of criteria is used (List 1). The criteria are ordered by their priorities: that is Criterion 2 is calculated only if more than one pattern takes the same value for Criterion 1, Criterion 3 is calculated only if more than one pattern takes the same value for Criterion 2 (obviously for Criterion 1 as well) etc. **Each consecutive criterion is calculated only if more than one pattern takes the same value for the preceding criteria.**

List 1

Criterion 1	**The presence of asterisks ("*") in a pattern** The patterns without "*" have higher priority.
Criterion 2	**The number of matching digits/symbols** The more matching digits a pattern has, the higher its priority.
Criterion 3	**The number of square brackets ("[]")** The more ranges a pattern has, the higher its priority.
Criterion 4	**The number of question marks ("?")** The more question marks a pattern has, the higher its priority.
Criterion 5	**The number of braces ("{}")** The more ranges a pattern has, the higher its priority.
Criterion 6	**The number of asterisks ("*")** The fewer asterisks a pattern has, the higher its priority.
Criterion 7	**The value of the metric** The lower the metric of a pattern is, the higher its priority.
Criterion 8	**The position in the routing table** The higher the position of a pattern in the routing table is, the higher its priority.

The algorithm is discussed in the example below.

Example The user has dialed 1231 and Routing Agent has found the following list of matching patterns.

1. The list of matching patterns found by RA
2. *1*
3. 123*
4. {11-15}3*
5. ?2?1
6. 123?
7. [1-3]*
8. [1-3]???
9. {100-150, asd, *\?}1
10. 12*31
11. 1[1-3]3[0-8]
12. 1231
13. *2*1
14. *

The step by step discussion of the **Best Matching Algorithm** is as follows.

Step 1: The list is split into two groups separating the patterns with "*" from the ones without (Criterion 1). The patterns with "*" form a group with lower priority and are pushed back to the end of the list (Table 1).

15.	**Table 1**
16.	**The list split into two subgroups**
17.	?2?1
18.	123?
19.	[1-3]???
20.	{100-150, asd, *\?}1
21.	1[1-3]3[0-8]
22.	1231
23.	*1*
24.	123*
25.	{11-15}3*
26.	[1-3]*
27.	12*31
28.	*2*1
29.	*

Step 2: The two groups of the patterns are sorted digits in descending order (Criterion 2, Table matching digits are grouped into sub-lists its position and does not participate in further separately from each other by the number of matching 2). The patterns that have the same number of (Table 3). If a sub-list consists of one pattern, it stays in discussions.

Table 2

30.	The list of patterns	31.	Criterion 2
32.	1231	33.	4
34.	123?	35.	3
36.	?2?1	38.	2
37.	1[1-3]3[0-8]	39.	2
40.	{100-150, asd, *\?}1	41.	1
42.	[1-3]???	43.	0
44.	12*31	45.	4
46.	123*	47.	3
48.	*2*1	49.	2
50.	*1*	52.	1
51.	{11-15}3*	53.	1
54.	[1-3]*	56.	0
55.	*	57.	0

Table 3

58.	The list of patterns	59.	Criterion 2
60.	1231	61.	4
62.	123?	63.	3
64.	?2?1	66.	2
65.	1[1-3]3[0-8]	67.	2
68.	{100-150, asd, *\?}1	69.	1
70.	[1-3]???	71.	0
72.	12*31	73.	4
74.	123*	75.	3
76.	*2*1	77.	2
78.	*1*	80.	1
79.	{11-15}3*	81.	1
82.	[1-3]*	84.	0
83.	*	85.	0

The principle by which the patterns have been sorted in Step 1 is applied in all further steps with a different criterion.

Step 3: Each sub-list is sorted separately from the others by the number of square brackets (**"[ ]"**) in the pattern in descending order (Criterion 3, Table 4). The patterns that have the same number of ranges are grouped into sub-lists (Table 5). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 4

86.	The list of patterns	87.	Criterion 3
88.	1231	89.	-
90.	123?	91.	-
92.	1[1-3]3[0-8]	94.	2
93.	?2?1	95.	0
96.	{100-150, asd, *\?}1	97.	-
98.	[1-3]???	99.	-
100.	12*31	101.	-
102.	123*	103.	-
104.	*2*1	105.	-
106.	*1*	108.	0
107.	{11-15}3*	109.	0
110.	[1-3]*	112.	1
111.	*	113.	0

Table 5

114.	The list of patterns	115.	Criterion 3
116.	1231	117.	-
118.	123?	119.	-
120.	1[1-3]3[0-8]	121.	2
122.	?2?1	123.	0
124.	{100-150, asd, *\?}1	125.	-
126.	[1-3]???	127.	-
128.	12*31	129.	-
130.	123*	131.	-
132.	*2*1	133.	-
134.	*1*	136.	0
135.	{11-15}3*	137.	0
138.	[1-3]*	139.	1
140.	*	141.	0

Step 4: Each sub list is sorted separately from the others by the number of question marks in the pattern in descending order (Criterion 4, Table 6). The patterns that have the same number of question marks are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 6

142.	The list of patterns	143.	Criterion 3
144.	1231	145.	-
146.	123?	147.	-
148.	1[1-3]3[0-8]	149.	-
150.	?2?1	151.	-
152.	{100-150, asd, *\?}1	153.	-
154.	[1-3]???	155.	-
156.	12*31	157.	-
158.	123*	159.	-
160.	*2*1	161.	-
162.	*1*	164.	0
163.	{11-15}3*	165.	0
166.	[1-3]*	167.	-
168.	*	169.	-

Step 5: Each sub-list is sorted separately from the others by the number braces (**"{ }"**) in the pattern in descending order (Criterion 5, Table 7). The patterns that have the same number of ranges are grouped into sub-lists (Table 8). If a sub-list consists of one pattern it stays in its position and does not participate in further discussions.

Table 7

170.	The list of patterns	171.	Criterion 4
172.	1231	173.	-
174.	123?	175.	-
176.	1[1-3]3[0-8]	177.	-
178.	?2?1	179.	-
180.	{100-150, asd, *\?}1	181.	-
182.	[1-3]???	183.	-
184.	12*31	185.	-
186.	123*	187.	-
188.	*2*1	189.	-
190.	{11-15}3*	192.	1
191.	*1*	193.	0
194.	[1-3]*	195.	-
196.	*	197.	-

Table 8

198.	The list of patterns	199.	Criterion 4
200.	1231	201.	-
202.	123?	203.	-
204.	1[1-3]3[0-8]	205.	-
206.	?2?1	207.	-
208.	{100-150, asd, *\?}1	209.	-
210.	[1-3]???	211.	-
212.	12*31	213.	-
214.	123*	215.	-
216.	*2*1	217.	-
218.	{11-15}3*	219.	1
220.	*1*	221.	0
222.	[1-3]*	223.	-
224.	*	225.	-

Step 6: This step is applicable to the subgroup containing patterns with "*", the group with lower priority. Each sub-list is sorted separately from the others by the number of asterisks ("*") in ascending order (Criterion 6). The patterns that have the same number of asterisks are grouped into sub-lists. If a sub-list consists of one pattern it stays in its position and does not participate in further discussions.

Step 7: Each sub-list is sorted separately from the others by the value of metric in ascending order (Criterion 7). The patterns that have the same value of metric are grouped into sub-lists. If a sub-list consists of one pattern it stays in its position and does not participate in further discussions.
The values of metrics are taken from the routing table.

Step 8: The patterns in each sub-list are arranged by their positions in the routing table (Criterion 8).

The subgroup containing patterns with "*" is attached to the end of the subgroup without "*" forming a single list of sorted patterns. The obtained list is the sorted list of the patterns by the Best Matching Algorithm (Table 9).

226.   Table 9
227.   The sorted list of patterns
228.   1231
229.   123?
230.   1[1-3]3[0-8]
231.   ?2?1
232.   {100-150, asd, *\?}1
233.   [1-3]???
234.   12*31
235.   123*
236.   *2*1
237.   {11-15}3*
238.   *1*
239.   [1-3]*
240.   *

VoIP Carrier Wizard

VoIP Carrier Wizard is used to define access codes for available VoIP Carrier account which will particularly allow to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

For each configured VoIP carrier, wizard creates specific IP-PSTN routing rule in the Call Routing table. Additionally, a virtual extension will be automatically generated in Extensions Management will be registered on the defined VoIP Carrier's SIP server and on behalf of which the calls from Quadro's users towards the created VoIP Carrier will be placed.

VoIP Carrier Wizard – Page 1 provides a possibility to describe VoIP carrier:

When **Vonage** is selected in **VoIP Carrier** drop down list, SIP Server and Port will be already predefined in the next page. **Manual** selection allows to set up the VoIP Carrier settings manually.
Description field allows to insert an optional description of the VoIP Carrier.

Fig. II-116: VoIP Carrier Wizard page

VoIP Carrier Wizard – Page 2 is used to define VoIP Carrier Settings. Page contains following components:

1. VoIP Carrier Common Settings
Account Name text field requires a username for authentication on the defined SIP server.
Password requires a password for authentication on the defined SIP server.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error will appear: "Incorrect Password confirm".

SIP Server text field requires an IP address or the hostname of the SIP server destination party is registered on.
SIP Server Port text field requires the port number of the SIP server destination party is registered on.

2. VoIP Carrier Advanced Settings
Use RTP Proxy checkbox is applicable only when route is used for calls towards configured VoIP Carrier from peer located outside the Quadro. When this checkbox is selected, RTP streams between external users will be routed through Quadro, otherwise, when checkbox is not selected, RTP packets will be moving directly between peers.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested for some SIP servers only, for others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If no reply is received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will be sent to it once again.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name), the port number of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

VoIP Carrier Wizard – Page 3 contains VoIP Carrier access code selection components:

Access Code text field requires a digit combination by dialing which the corresponding VoIP Carrier will be reached.

Route Incoming Calls To drop down list allows to select an extension (or Auto Attendant) on the Quadro where incoming calls from the configured VoIP Carrier should be routed to.

Failover to PSTN checkbox selection will route the call to PSTN through local FXO line in case if VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the <u>Call Routing</u> table maintaining digit transmission to local PSTN when IP call towards the configured VoIP Carrier cannot be established.

Please Note: Warning message will inform that the defined **Access Code** already exists in the Call Routing table or causes a conflict with entries already in the Call Routing table. In this case, when proceeding the **VoIP Carrier Wizard**, existing entry in the Call Routing table will be automatically overwritten by the new settings.

RADIUS Client Settings

The **RADIUS** (Remote Authentication Dial In User Service) specifies the RADIUS protocol used for authentication and authorization, to differentiate, to secure and to account for the users. The RADIUS Server gives an extra possibility for caller from/through Quadro to pass authentication to be able to dial the specific number.

When RADIUS client is enabled on the Quadro, any caller that dials routing pattern with **Authentication&Accounting** option selected (see Call Routing table), will primarily pass authentication locally, through **Local AAA Table**, and if local authentication failed, will pass additional authentication on the RADIUS Server. This can be accomplished by caller's number automatic detection or a customizable login prompt, where caller is expected to enter username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an insecure network could determine a user's password. If no response from the RADIUS Server is returned after Receive Timeout expires, the request is resent a number of times, defined in the Retry Count list. The client also can forward requests to an alternate server or servers if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not have a shared secret must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the Quadro Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the Quadro.

Please Note: RADIUS Client cannot be disabled if there is at least one route with **Authentication&Accounting** or **Accounting** value configured in the **AAA Required** drop down list at the Call Routing table. To be able to disable the RADIUS Client on the Quadro, appropriate routes should be remove first.

The other RADIUS Client settings are divided into three groups:

1. Registration Settings
Primary Server requires the IP address of the primary Radius Server.
Secondary Server requires the IP address of the secondary Radius Server.
NAT Station IP text fields require the NAT PC WAN IP address. If no NAT Station is specified here, Quadro's IP address will be sent to the RADIUS server.
Secret Key is used to insert the secret key between the Radius client and the server. Contact the Radius server administrator to get the secret key for your Quadro.
Confirm Secret Key field is used to verify the secret key. If the entered **Secret Key** does not correspond to the one in the **Confirm Secret Key** field, the error will appear: "The Secret Key does not match. Please try again".
Retry Count allows selecting the number of attempts before canceling the registration.
Receive Timeout allows selecting the timeout (in seconds) between two attempts to register.
Encoding Type allows selecting the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type also should be requested from the Radius Server administrator.
The **Authorization Port** text field requires the port number on the RADIUS server where Quadro will send the authentication requests.
The **Accounting Port** text field requires the port number on the RADIUS server where Quadro will send the accounting messages.

Fig. II-117: Radius Client Settings page

1. **Authentication Settings**

Enable common login for all users in time of by Phone authentication checkbox enables custom settings for the callers passed an authorization by phone on the Quadro. Checkbox enables **Username** and **Password** text fields to insert the custom settings that will stand instead of source caller's settings when being delivered to the RADIUS server.

Authentication on Destination RADIUS Server parameters group is used to insert a **Username** and a **Password** (followed by the password confirmation) used by PSTN callers to pass the authentication on to the RADIUS Server of the destination Quadro. If these fields are left empty, the original authentication settings that PSTN users enter for authentication will be used.

3. **Accounting Settings**

The **Username** field is dedicated for accounting service only and is used to insert an identification username accounting will be performed on behalf of. When no username is specified in this field, source username will be used for accounting.

Send Accounting messages manipulation radio buttons group is used to select the whether both **Start** and **Stop** Accounting messages should be sent or **Stop** Accounting message is delivered only.

Voice Mail Common Settings

The **Voice Mail Common Settings** page is used to configure the Voice Mail recording codec.

The page consists of the **Recording Codec** drop down list contains the existing codecs for voice mail compression. Changing the Voice Mail recording codec will directly affect the allocated memory size for users.
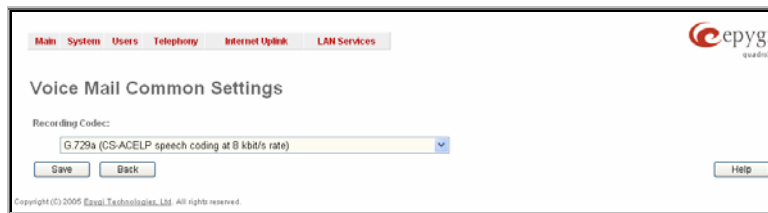
Fig. II-118: Voice Mail Coming Settings page

Dial Plan Settings

The **Dial Plan Settings** page is used to adjust the dialing timeouts for the routing calls over Quadro.

This page consists of the only drop down list used to configure the dialing timeout for the Routing calls. Values selected in the lists indicate the interval between the dialed number and it being applied to the network.
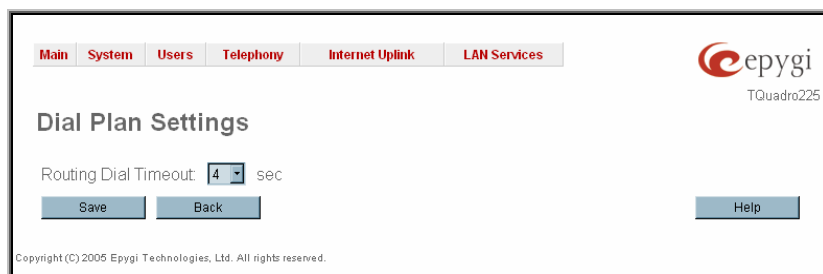
Fig. II-119: Dial Plan Settings page

Internet Uplink Menu

Fig. II-120: Internet Uplink menu in Dynamo theme
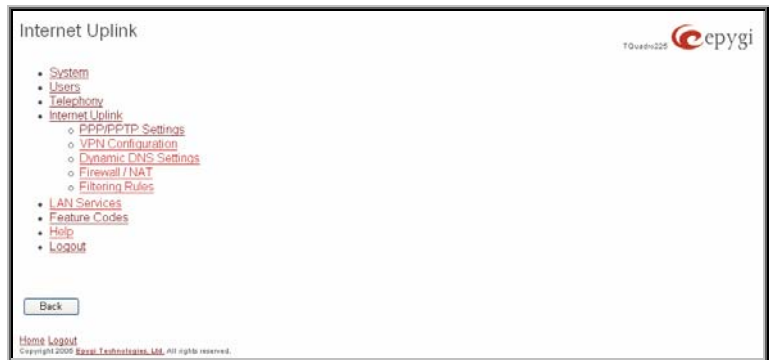
Fig. II-121: Internet Uplink menu in Plain theme

PPP/ PPTP Settings

The **PPP/PPTP Settings** page is used to establish a connection over the DSL link or any other type of uplink, to the ISP (provider party). A connection is needed to set up and to make or receive calls through PPP over Ethernet. The connection may be configured for manual setup or to be always up. Once a connection has been established between the Quadro and the provider, Quadro users will be able to make and receive calls at any time.

The **PPP/PPTP Settings** page offers the following components:

Advanced PPP Settings link refers to same named page where certain parts of the negotiation process during connection establishment can be adjusted. Link is not available when accessing this page through Internet Configuration Wizard.

PPTP Server text fields are only enabled when Quadro is running with the PPTP interface and require the IP address of the PPTP server.

Encryption drop down list is only enabled when Quadro is running with the PPTP interface and is used to select the encryption for the traffic over the PPTP interface.

Authentication Settings require the Username and the Password used for the authentication on the ISP server.

Dial Behavior radio buttons:

- **Dial Manually** - if this radio button is activated, a button will be displayed in the main management window that serves to switch the Internet connection on/off. When accessing the Internet, every station of the connected LAN has to connect to Quadro first.
- **Always connected** - Quadro stays in the always connected mode. This will allow remaining always online in the network.

IP Address Assignment radio buttons are used to define the way of IP address assignment for the PPP interface:

- **Dynamic IP Address** – the IP address to the PPP interface will be assigned dynamically by the DHCP server.
- **Fixed IP Address** – the fixed user defined IP address will be assigned to the PPP interface.

Keep Connection alive checkbox enables keeping the connection alive by sending control packets dedicated for the link state verification.
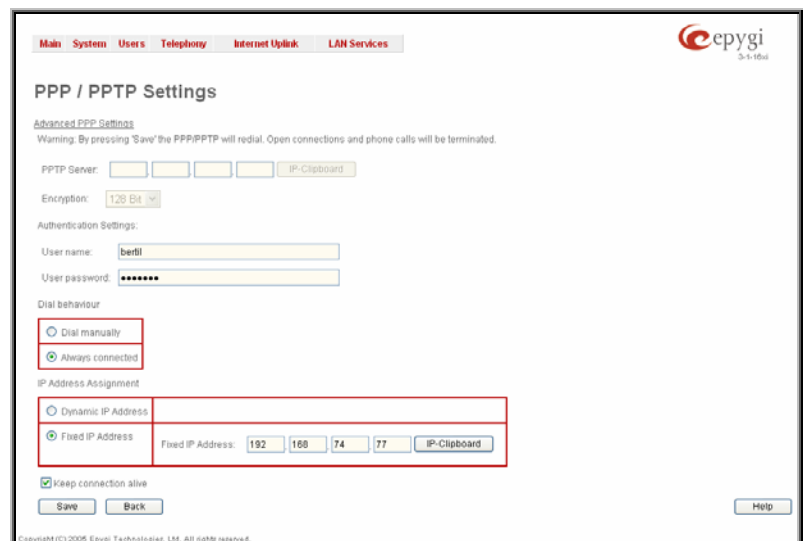
Fig. II-122: PPP Dial Settings page

Advanced PPP Settings

The **Advanced PPP Settings** are used to enable/disable certain parts of the negotiation process during connection establishment. These settings are available only if Quadro has a PPPoE WAN interface.

Attention: Disabling any of the services below may cause problems when establishing a connection up to complete connection failure. The default settings should be changed only if the ISP (Internet Service Provider) requires it explicitly or if the peer system has problems with one of the services listed below. More information about these services can be found at: http://www.protocols.com/pbook/ppp.htm.

The **Advanced PPP Settings** page offers a group of checkboxes:

Enable automatic PPP restart at checkbox is used to select the time when PPP connection will be automatically restarted. Checkbox selection enables **LCP echo failures** text field that indicates the number of LCP echo failure packets received before the PPP connection will be considered as dead and will be restarted.

Disable CCP (Compression Control Protocol) negotiation - this option should only be selected if the peer system is not working properly, e.g., not accepting the requests from the PPPD (Point-to-Point Daemon) for CCP negotiation.

Disable magic number negotiation - with this option, PPPD cannot detect a looped-back line. This option should only be selected if the peer is not working properly.

Disable protocol field compression negotiation in both the receive and the transmit direction - no protocol field compression will take place.

Disable Van Jacobson style TCP/IP header compression in both the transmit and the receive direction - no negotiation of TCP/IP header compression will take place, the header will always be sent uncompressed.

Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression - with this option, PPPD will not compress the connection-ID byte from Van Jacobson, nor ask the peer to do so.

Disable the IPXCP and IPX protocols - this option should only be selected if the peer is not working properly and cannot handle requests from PPPD for IPXCP negotiation.
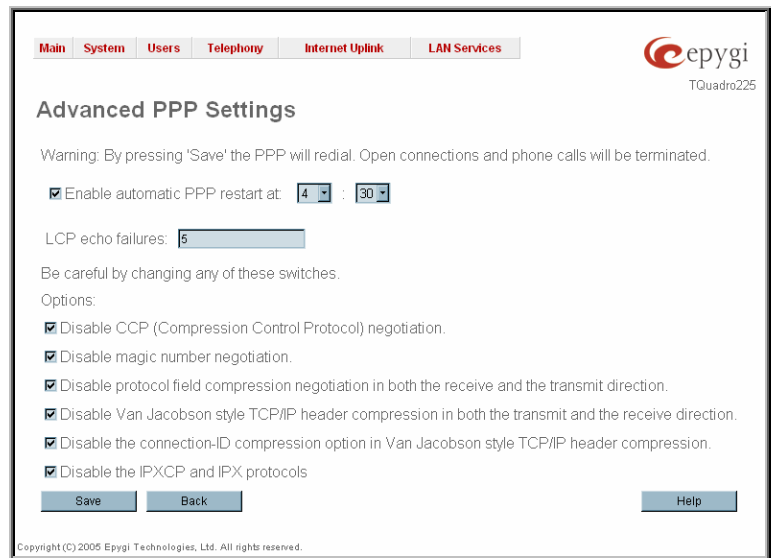
Fig. II-123: Advanced PPP Settings page

VPN Configuration

A **VPN (Virtual Private Network)** is established to connect two local networks (intranets) over the Internet securely. VPN routers manage authentication between servers and clients and handle data encryption for the connection. Only authorized users may access the network, and the data exchange cannot be intercepted.

VPN connections are, in many ways like every Internet connection;, they are based on IP addresses, which means, the concerned VPN gateways must authenticate the IP addresses of their respective partner's VPN gateways. Each time a specific VPN is to be established, usually, the same IP addresses are expected,. That fact won't cause any problems if both VPN partners have fixed WAN IP addresses. But, there may be good reasons to prefer dynamically allocated IP addresses. To enable devices that use a variable IP address to become part of a VPN, they are turned into so-called Road Warriors. Then they are able to reach their corporate network via authentication at the company's VPN gateway device, for example. This VPN gateway device has to have a fixed IP address for Internet access, because every VPN needs at least one VPN gateway with a fixed IP address.

The partner devices of a VPN must have different WAN IP addresses, and if they are connected to local area networks, these LAN's must have different IP addresses. As all Quadro devices have the same default IP addresses on delivery, at least one of them must be reconfigured in order to set a new IP addresses.

Quadro supports several kinds of VPN connections such as **IPSec**, **L2TP** and **PPTP**.

The **VPN Configuration** page offers four links (IPSec Configuration, PPTP Client Configuration, PPTP Server Configuration and L2TP Configuration), which leads to the corresponding feature settings pages.

Attention: It is strongly recommended not to run different kinds of VPN tunnels between the same endpoints simultaneously.
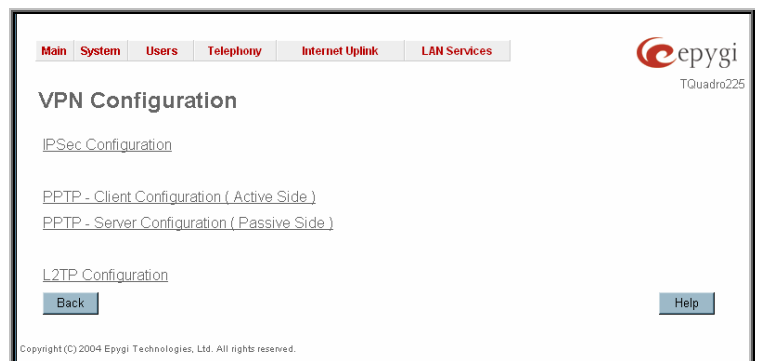
Fig. II-124: VPN Configuration page

An IPSec connection includes authentication and encryption to protect data integrity and confidentiality. VPNs are "virtual" in the sense that individuals can use the public Internet as a means of securely accessing an internal network. Once the IPSec connection is established, users have access to the same network resources, addresses, and so forth as if they were connected locally. VPNs are "private" because the data is encrypted between two VPN gateways. Encryption makes it very difficult for anyone to intercept data and capture sensitive information such as passwords. The Quadro can be set up to act as a VPN router when connected to the Internet with a fixed IP address or as an IPSec connection Road Warrior when using dynamic IP addresses.

Establishing an IPSec connection normally requires the functionality of a VPN gateway on each side of the communication line. An intelligent Internet access router, for example Quadro, delivers this function but also PCs or workstations may be equipped with VPN gateway functionality. For home offices it may be too expensive to get fixed IP addresses so they prefer dynamically allocated IP addresses.

When Quadro is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. Then Quadro is prepared to establish an IPSec connection with another VPN gateway device, but allows access to Road Warriors, too. A traveling salesperson's notebook for example could be such a Road Warrior. Access to their company's intranet via IPSec connection can be obtained regardless of location.

Besides being a VPN gateway, Quadro can be set up to act as a Road Warrior. If a home office for example is connected to the Internet via Quadro with PPPoE (Point-to-Point Protocol) and dynamic IP addressing, setting up Quadro as a Road Warrior will allow a IPSec connection to the corporate network.

For the encryption and decryption of the data transmitted via the IPSec connection, a key is used. **RSA** used by Quadro is an asymmetric key system. It has to be available on both sides of the IPSec connection and will generate a different pair of keys on each side, a private and a public key. During the connection establishment, some data is encrypted with the remote party's public key and can be decrypted with their private key by themselves and vice versa (the data encrypted there with Quadro's public key can be decrypted with Quadro's private key). Since the private key is never transmitted in any way, it stays completely unknown for everybody, thus the system remains safe. Even if someone gets hold of the public key, decryption cannot be possible without the private key. Quadro generates such a pair of keys automatically when it is set up. The user cannot see the private key, but must know the public one, as their IPSec connection partner will need it.

Please Note: Always a pair of keys will be generated, a public one and a private one, the former pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

The **IPSec Configuration** link refers to the **IPSec Connection Settings** page, which gives an overview of all existing IPSec connections characterized by their **Connection Name**, the **Remote Gateway** (the IP address or the hostname of the IPSec connection partner), the **State** of the IPSec connection (Stopped, Connecting, Activated, Waiting or Connected) and the dedicated **Keying Type** (the encryption type). The content of the table can be sorted in ascending or descending order by clicking on the header of the respective column. There is a checkbox for every IPSec connection to select it for further editing.

Start activates the connection establishment of the selected IPSec connection. The **State** of the IPSec connection will change into "Connected" or "Activated" depending on the IPSec connection type. If no record is selected, the "One Record should be selected" error message occurs.

Attention: It is not recommended to start a static and a dynamic connection configured to use the same secret key simultaneously. A dynamic connection may capture the static connection peer and vice versa, depending on which connection established first.

Stop disconnects the selected IPSec connection. The state of the IPSec connection will change into "Stopped". If no record is selected, the "One Record should be selected" error message will occur. More than one record may be selected at a time to be stopped.

Fig. II-125: IPSec Connection Settings page

Add leads to the **Add IPSec Connection** wizard where a new IPSec connection can be defined and specified. The wizard provides several pages.

Edit leads to a set of **IPSec Connection Properties** pages to modify the parameters of the selected IPSec connection. The page includes the same components as the **Add IPSec Connection** page. To operate with **Edit**, only one record may be selected, otherwise an error will occur: "One row must be selected".

Restart all Connections restarts all active IPSec connections. The **State** of these IPSec connections will turn into **Connected** or **Activated** if the restart procedure has been completed successfully.

RSA Key Management leads to the **RSA Key Management** page to see the current RSA key, to generate a new one and to send it to the peer via e-mail.

The first IPSec Connection Wizard page **Add IPSec Connection** has the **Connection Name** text field that requires a new IPSec connection name, which is mandatory, and should be filled out, otherwise an error will occur: "Error: Incorrect connection name".

Please Note: The input in the **Connection Name** field should be only in Latin characters, otherwise an error occurs and no IPSec connection can be created.

The **Peer type** drop down list is used to choose the remote machine type for the IPSec Connection to be established. If the list does not include the required type of machine, choose **Other**.

VPN Network Topology drop down list allows to select the location of the peers participating to the VPN connection. Following selections are present in the list:

- Quadro<>Peer – direct connection between Quadro and a peer.

- Quadro<>[Internet]<>Peer – connection between Quadro and peer over Internet.

- Quadro<>NAT<>[Internet]<>Peer – connection between Quadro and peer over Internet through Quadro provider's NAT.

- Quadro<>[Internet]<>NAT<>Peer – connection between Quadro and peer over Internet through peer provider's NAT.

Fig. II-126: IPSec Connection Wizard - Add IPSec Connection

The second page of the IPSec Connection Wizard, **IPSec Connection Properties** serves to specify the members of the IPSec Connection and to set the basic parameters for encryption.

A group of radio buttons are used with **Dynamic IP/Road Warrior** and **Static IP/ Remote Gateway** to select if the remote Quadro (or another VPN gateway device) is connected to the Internet with a dynamic IP address and is acting as a **Road Warrior**, or is connected to the Internet with a fixed IP address and is acting as a **VPN Gateway**.

If **Dynamic IP / RoadWarrior** is selected, the **Remote Gateway IP Address** text field automatically will get the value "any", to allow access independent from the sending IP address.

Selecting **Static IP / Remote Gateway** requires entering the IP address or the hostname of the remote Quadro (or another VPN gateway device) in the **Remote Gateway** text field.

Please Note: **Static IP/ Remote Gateway** selection is not possible if this Gateway is positioned behind NAT, since the IP-address of the remote gateway is not reachable directly in this case.

Quadro <> Remote Gateway allows access from the local Quadro to the remote VPN gateway (local subnet and remote subnet are not included). This includes management access. Checkbox is disabled when "Quadro<>NAT<>[Internet]<>Peer" or "Quadro<>[Internet]<>NAT<>Peer" is selected from **VPN Network Topology** drop down list on the first page of **IPSec Connection Wizard**.

Local Subnet <> Remote Gateway allows access from all stations connected to the local network to the remote VPN gateway device (local Quadro and remote subnet are not included). Checkbox is disabled when "Quadro<>[Internet]<>NAT<>Peer" is selected from **VPN Network Topology** drop down list on the first page of **IPSec Connection Wizard**.

Fig. II-127: IPSec Connection Wizard -IPSec Connection Properties

Quadro <> Remote Subnet allows access from the local Quadro to all stations of the remote LAN (local subnet and remote VPN gateway devices are not included). Checkbox is disabled when "Quadro<>NAT<>[Internet]<>Peer" is selected from **VPN Network Topology** drop down list on the first page of **IPSec Connection Wizard**.

Local Subnet <> Remote Subnet allows access from all stations of the local network to all stations of the remote LAN (VPN gateway devices are not included). In this case the local and remote subnet IP addresses and subnet masks have to be entered in the corresponding text fields **Local Subnet IP** and **Remote Subnet IP**.

More than one of the above checkboxes may be selected to specify the desired communication relations.

The **Stop Connection if not successful** checkbox allows to stop the IPSec connection attempts if the partner is still unreachable after the timeout period. If the checkbox is unselected, the system will continue to try to reach the IPSec connection partner.

The right side of the page offers security settings for key exchange, data encryption and authentication:

The area **Keying Type** offers the choice between automatic and manual keying. To use manual keying, the **Static IP / Remote Gateway** needs to be selected.

Auto Keying requires the **ESP** (Encapsulated Security payload) and **IKE** (Internet Key Exchange) settings (in addition with **Diffie-Helman Group** settings) to be selected for the automatic keying exchange. **Encryption** and **Authentication** parameters should be defined for each of these standards, as well as for the **Manual Keying**.

The **Encryption** drop down list offers the following standards for selection:

DES (Data Encryption Standard) is a block cipher algorithm with 64-bit blocks and a 56-bit key. This algorithm is considered to be insecure for sensitive information.

3DES (Triple DES) uses three DES encryptions on a single data block with three different keys to achieve a higher security than is available from a single DES pass.

AES (Advanced Encryption Standard) is a computer security standard, which became effective on May 26, 2002 by NIST to replace DES. The cryptography scheme is a symmetric block cipher, which encrypts and decrypts 128-bit blocks of data. Lengths of 128, 192, and 256 bits are standard key lengths used by AES.

The area **Authentication** offers the following parameters to be selected:

SHA (Secure Hash Algorithm) is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPSEC.

SHA1 is an enhanced version of SHA. It works with checksums like MD5 does, but it makes a longer hash.

MD5 (Message Digest) is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.

The **Diffie-Hellman** parameter is used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group, which is based upon the prime numbers.

Group 2048 (high) is stronger (more secure) than Group 2 (medium), which is stronger than Group 1 (low). Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, and Group 2048 provides 2048 bits. If mismatched groups are specified on each peer, negotiation fails.

Depending on whether the automatic keying type or the manual one has been selected, the button **Next** will lead you to the **Automatic Keying** or **Manual Keying** page.

The third page of the IPSec Connection wizard, **Automatic Keying**, is used to setup a type of password (**Shared Secret**) or the **RSA** public key to secure your IPSec Connection. The functionality of **Perfect Forward Secrecy** (PFS) can be added to both.

Shared Secret is a type of password consisting of any characters that both of the IPSec Connection partners must know. The authentication will be done with this shared secret. All encryption functions below will remain concealed.

RSA requires the public RSA key of your IPSec Connection partner.

The **Local ID** requires an IP address, Quadro FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

Remote ID also requires an IP address, the IPSec Connection partner's FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

PFS (Perfect Forward Secrecy) is a procedure of system key exchange, which uses a long-term key and it generates a short-term keys as is required. Thus an attacker who acquires the long-term key can neither read previous messages that she may have captured nor read future ones.

Fig. II-128: IPSec Connection Wizard - Automatic Keying Settings page

Use IPSec Compression enables IPSec data compression. This option is displayed only if the IPSec-VPN partner supports it.

Fig. II-129: IPSec Connection Wizard - Manual Keying Settings page

The **Manual Keying** page offers the following components:

Depending on the selected encryption and authentication services of the prior page (IPSec Connection Properties) you will get some of the following text fields:

- **DES Encryption Key**
- **3DES Encryption Key**
- **SHA1 Authentication Key**
- **MD5 Authentication Key**

Manual keys must be entered in the hexadecimal format, otherwise the "Incorrect Encryption Key" error appears.

The **SPIs** (Security Parameter Index) are indices to keep the IPSec Connection tunnels distinct. A security association (SA) is defined by destination, protocol and SPI. Without the SPI, connections to the same gateway using the same protocol can not be distinguished.

The public key is displayed in the **RSA Public Key** text field so the user may inform their IPSec connection partner about it, for example, via fax.

Furthermore, the user has a possibility to generate a new pair of keys by specifying the key length with the corresponding radio buttons **Generate a new 1024bit RSA Key** and **Generate a new 2048bit RSA Key** and the clicking the **Generate** Button.

A valid RSA key should fit to following requirements:

- RSA key doesn't start with "0s"
- RSA key doesn't end with "=="
- RSA key contains symbols other than Alphanum, +, /, =

The **Email this to the peer** text field requires the mailing address of the IPSec connection partner. The **Send** button will insert Quadro's public RSA key into an e-mail and send it to the IPSec connection partner.

Fig. II-130: IPSec Connection Wizard - IPSec Connection RSA Key Settings page

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) is used to establish a virtual private network (VPN) over the Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers. PPTP encapsulates any type of network protocol (IP, IPX, etc.) and transports it over IP. Thus if IP is the original protocol, IP packets ride as encrypted messages inside PPTP packets running over IP. PPTP is based on point-to-point protocol (PPP) and the Generic Routing Encapsulation (GRE) protocol. Encryption is performed by Microsoft's Point-to-Point Encryption (MPPE), which is based on RC4.

L2TP (Layer **2 T**unneling **P**rotocol) is a protocol from the IETF, which allows a PPP session to run over the Internet, an ATM, or frame relay network. L2TP does not include encryption (as does PPTP), but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP network server (LNS) at the corporate side. Large carriers also may use L2TP to offer remote POPs to smaller ISPs. Users at the remote locations dial into the modem pool of an L2TP access concentrator, which forwards the L2TP traffic over the Internet or private network to the L2TP servers at the ISP side, which then sends them on to the Internet.

For **PPTP and L2TP Connections**, two parties are required: a **Client** and a **Server**. The client is responsible for establishing the connection, hence active. The server is waiting for clients; it is not able to initiate the connection itself, hence passive.

Attention: L2TP tunnels have no data encryption mechanism.

The **Host Name** and a **Password** specify each side. The client should know the server's name and password (the Quadro server has no password) and the server should set the client's host name and a password. The client and server settings have to match on both sides for successful connection establishment.

Clients and Servers are identified by their hostnames, which means that only one client can be connected to the server in the same network. Servers also define the range of IP addresses that are assigned to the Server and Client hosts participating in a connection.

The **PPTP Client Configuration** link displays a page where all existing PPTP client connections are listed, characterized by their **Connection Name**, the **State** of the PPTP connection (Pending, Disabled, Trying…, Authentication Failure, No Connectivity - still trying, Unknown, Broken, or Connected) and the **Remote IP/Hostname** (the IP address or the hostname of the PPTP server). PPTP Connections' states, except the "Disabled" state, are established as a link that refers to the page where logout information about PPTP connection status is displayed. Logs can be useful to determine problems on PPTP connections failure.

Start initiates the PPTP client(s) activity (reaching the server). Several client connections may be selected at once.

The **Stop** button is used to stop the selected PPTP client(s) activity. Several client connections may be selected at once using this function.

Fig. II-131: PPTP Client Configuration page

Add leads to the **PPTP Client Connection - Add Entry** page where a new PPTP client connection can be established:

Server Host Name requires the server's hostname.

Please Note: The input in the **Server Host Name** field should be only in Latin characters, otherwise an error occurs and no PPTP connection can be created.

Client Host Password requires the local peer password.

The **Server Host IP** radio buttons allow selecting the PPTP server.
IP requires the IP address of the PPTP server.
Hostname requires the FQDN (Full Qualified Domain Name) of the PPTP server.

Please Note: All settings should be configured the same way on both the PPTP client and server hosts, that is to say, for successful PPTP tunnel establishment; all settings should match each other.

Fig. II-132: PPTP Client Configuration - Add Entry page

The **PPTP Server Configuration** link displays a page to configure the PPTP server connections. It is divided into two pages with a table of the existing PPTP server connections on one page and the PPTP server settings on the other.

The page **PPTP Server Connections** offers the following input options:

The table **PPTP Server Connections** lists all the PPTP connections, characterized by their **Connection Name** and the **State** of the PPTP connection (Disabled, No Client Connected or Connected: IP address). Each PPTP Server connection can hold only one PPTP tunnel.

Start is used to activate the selected PPTP connection(s). Several server connections may be selected at once.

Stop is used to deactivate the selected PPTP connection(s). Disabling the connection will disconnect all connected clients and close the PPTP tunnel. Several server connections can be selected at once to operate with this function.

Fig. II-133: PPTP Server Configuration page

Add leads to the **PPTP Server Connection - Add Entry** page where a new PPTP Server connection can be made.

Client Host Name and **Client Password** require the corresponding client's host name and password.

Please Note: The input in the **Client Host Name** field should be only in Latin characters, otherwise an error occurs and no PPTP connection can be created.

In certain cases, **Client Host Name** can be a conditional username defined by the client and used for PPTP connection establishment.

Please Note: All settings should be configured the same way on both the PPTP client and server, that is to say, for successful PPTP tunnel establishment, all settings should match.

Fig. II-134: PPTP Server Configuration - Add Entry page

The **PPTP Server Configuration** page is used to configure the PPTP server settings and offers the following components:

The **PPTP Subnet** text fields are used to enter the IP address range for the PPTP server and clients within the PPTP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the PPTP connection.

Please Note: The first address specified in the PPTP Subnet will be assigned to the PPTP server; others will be assigned to the clients. PPTP server subnet should be different from the L2TP server subnet, otherwise a corresponding error message appears.

Fig. II-135: PPTP Server Configuration page

The **L2TP Configuration** link displays a page to configure the L2TP connections.

Attention: L2TP tunnels have no data encryption mechanism.

The **L2TP Configuration** page has two pages with the table of existing L2TP connections on one page and the L2TP server settings on the other page.

The **L2TP Connections** page has the following components:

The **L2TP Connections** table lists all the L2TP connections characterized by their **Connection Name**, connection **Type** (active or passive), the **State** of the L2TP connection (Waiting, Connected, Trying, Disabled or Down) and the **Remote IP** address (the IP address or the hostname of the L2TP partner if connection is active). Each L2TP passive connection can hold only one L2TP tunnel.

Start is used to enable the selected L2TP server or client connection(s). Several records may be selected at with this function.

Stop is used to disable the selected L2TP server or client connection(s). Stopping the server will disconnect all connected clients and close the L2TP tunnel. Several records may be selected at once with this function.

Add leads to a page where the connection type (active or passive) has to be selected. Afterwards the appropriate **Add L2TP Connection** page will be displayed where a new L2TP connection can be established.

The **Passive L2TP Connection - Add Entry** page is used to specify passive L2TP server connections.

Client Host Name and **Client Password** text fields require the corresponding client's host name and password.

Please Note: The input in the **Client Host Name** field should be only in Latin characters, otherwise an error occurs and no L2TP connection can be created.

In certain cases, **Client Host Name** can be a conditional username defined by the client and used for L2TP connection establishment.

Fig. II-136: L2TP Configuration page

Fig. II-137: L2TP Configuration - Add Passive Connection page

Please Note: All settings on this page should be configured in the same way on both the L2TP client and server, that is to say,. for successful L2TP tunnel establishment, all settings should match.

The **Active L2TP Connection - Add Entry** page is used to specify L2TP client connections and offers the following components:

The **Server Host Name** text field requires the L2TP server's name.

Please Note: The input in the **Server Host Name** field should be only in Latin characters, otherwise an error occurs and no L2TP connection can be created.

The **Client Host Password** text field requires the local peer password.

The **Server IP** text field requires the IP address of the L2TP server.

Please Note: All settings have to be configured the same way both on the L2TP client and the server hosts. For successful L2TP tunnel establishment all the settings should match each other.

Fig. II-138: L2TP Configuration - Add Active Connection page

The **Configuration** page is used to configure the L2TP server settings and provides the following input options:

The **L2TP Subnet** text fields are used to enter the IP address range for the L2TP server and clients within the L2TP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the L2TP connection.

Please Note: The first address specified in the L2TP Subnet will be assigned to the L2TP server; others will be assigned to the clients. L2TP server subnet should be different from the PPTP server subnet, otherwise a corresponding error message appears.

Fig. II-139: L2TPServer Configuration page

To Specify an IPSec Connection

1. Press the Add button on the **IPSec Connection Settings** page. The **IPSec Connection Wizard** will appear in the browser window.
2. Select a VPN **Peer Type** and assign a name to the **IPSec Connection**. Press **Next** to go to the next page of the IPSec Connection wizard.
3. Enter the remote side IP parameters, check subnets/gateways for the connection, select the NAT traversal option (if needed), and the desired keying type. Press **Next** to advance to the next page of the IPSec Connection wizard.
4. If the **Automatic Keying** type has been selected enter the automatic keying parameters and select the PFS and IPSec compression options (if needed). If the **Manual Keying** type has been selected enter the encryption and authentication keys and SPI(s).
5. To specify an IPSec connection with these parameters press **Finish**. Use **Cancel** to abort the operation.

To Manage an RSA key for the IPSec Connection

1. Press the **RSA Key Management** button on the **IPSec Connection Settings** page. The **IPSec Connection RSA Key** will appear in the browser window.
2. Select the RSA key length and press **Generate** to generate a new RSA public key. This may take several seconds.
3. Enter a destination e-mail address in the **Email this key to peer** text field, then press **Send** to send the new RSA public key.

To Specify a PPTP Client Connection

1. Press the **Add** button on the **PPTP Client Configuration** page.
2. Enter the server host name in the **Server Host Name** text field.
3. Specify the PPTP client password in the **Client Password** text field.
4. Using the radio buttons on the page, select the server address representation (IP address or hostname) and provide the corresponding information in the **Server Host IP** fields.
5. Press **Save** to add a PPTP connection with these settings.

To Add a PPTP Server Connection

1. Press the **Add** button on the **PPTP Server Configuration** page.
2. Enter the client host name and the password in the **Client Host Name** and **Client Password** text fields.
3. Press **Save** to add a PPTP connection with these settings.

To Add an Active L2TP Connection

1. Press the **Add** button on the **L2TP Configuration** page.

2. Select the **Active Connection** link.
3. Enter the server host name in the **Server Host Name** text field.
4. Specify the L2TP client password in the **Client Password** text field.
5. Specify the server's IP address in the **Server IP** text field.
6. Press **Save** to add an active L2TP connection with these settings.

To Add a Passive L2TP Connection

1. Press the **Add** button on the **L2TP Configuration** page.
2. Select the **Passive Connection** link.
3. Enter the client host name and the password in the **Client Host Name** and **Client Password** text fields.
4. Press **Save** to add a passive L2TP connection with these settings.

To Delete/Stop/Start/Enable/Disable a VPN Connection

1. Select one or more checkboxes of the corresponding connections that ought to be deleted/stopped/started from the **Connection** tables. Press **Select all** to delete/stop/start all connections.
2. Click on the Delete/Stop/ Start button from the table's menu to perform the corresponding operation for the selected VPN connection(s).
3. If deleting confirm it with **Yes**. The VPN connection will be deleted. To abort the deletion and keep the VPN connection in the list, click **No**.

Dynamic DNS Settings

The **Dynamic DNS** (DynDNS) is a service that is used to map a dynamic IP address to a host name. Thus this service only makes sense if you are connected to the Internet with a dynamic IP address (and PPP, DHCP client) and want to allow access from the Internet to a device behind the firewall. For example, if you want to run your own WEB server.

To enable the DynDNS service on Quadro you first have to choose a DynDNS provider and register at their website.

The **Dynamic DNS Settings** page provides the following components:

The **Enable Dynamic DNS** checkbox selection enables the dynamic DNS service.

The **User** text field requires the username specified during the registration at the DynDNS provider.

The **Password** text field requires the password specified during the registration at the DynDNS provider.

The **Max time between updates** text field requires entering the period between two updates (in hours). The values entered in these fields should be greater than 24, otherwise an error occurs: "Update interval times smaller than 24 hours are too small". Normally, whenever you set up a connection to the Internet, the DynDNS is updated at least once in the period indicated in this field.

The **Use predefined service** radio button leads to the manual configuration of the DynDNS service. The selection enables the following optional settings:

The **Service** drop down list contains the provider list where the administrator needs to select the one that has been subscribed to.

The **Host** text field requires the name of the host on the Internet.

The **TZO Connection Type** text field is used for a special parameter required by the DynDNS provider TZO.

The **DHS Cloak-Title** text field is used for a special parameter required by the DynDNS provider DHS.

The **Mail Exchange** text field requires the address of the e-mail server where the DynDNS service provider will relay your e-mails.
Attention: If this service is used, make sure, that there is port forwarding configured for SMTP (port 25) to the internal e-mail server.

The **easyDNS Partner** text field is used for a special parameter required by the DynDNS provider easyDNS.

Fig. II-140: Dynamic DNS Settings page

Selecting the **Create Custom HTTP GET Request** radio button switches to the custom settings of the DynDNS service. Normally, the DynDNS provider uses HTTP get requests to map dynamic IP addresses to host names. If the user knows this HTTP get request exactly, the radio button **Create Custom HTTP GET Request** together with the text field **URL** allows to enter it directly.

The selection enables the following optional settings:

The **URL** text field requires the complete request to be sent to the DynDNS server. Normally it has the format:

[http://]www.server.domain:port/scriptpath/scriptname?param1=value1&param2=value2

The request modifies the nameserver database so that the hostname will be resolved to the new IP address.

The **Basic Authentication** checkbox enables the encoding of the username and password entered in the text fields above, and then uses the **Basic Authentication** method to notify the provider about the user authentication settings.

Most of the DynDNS providers require an authentication for security. The user can do that either together with the HTTP get request in the text field **URL** or by selecting the **Basic Authentication** checkbox.

Firewall and NAT

The **Firewall Configuration** page allows setting up a firewall, configuring the security level and enabling the NAT service of Quadro.

A **Firewall** is a security service configured by the Quadro administrator based on various criteria. The firewall allows or blocks traffic based on policies, services and/or IP addresses. The firewall has several levels of security policies (low, medium or high). The administrator may add additional service-based rules. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level.

NAT (Network Address Translation) is used to allow Quadro LAN members to connect to the Internet, using Quadro's WAN IP address. The Quadro/NAT also handles forwarding incoming packets from the WAN to the PCs or devices on Quadro's LAN.

The **Firewall Configuration** page offers the following components:

The **Enable NAT** checkbox selection enables Network Address Translation.

The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are:

- **Low Security** - Everything that is not explicitly forbidden is allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

Advanced Firewall Settings link refers to page where Quadro's privacy can be configured.

The **View Filter Rules** link opens the Filtering Rules page.
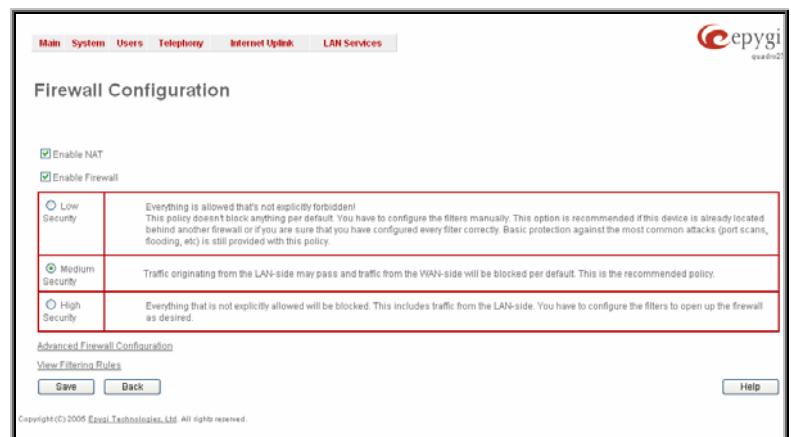
Fig. II-141: Firewall and NAT Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed toward the device. With these features enabled, Quadro will answer with inscrutable messages to the Ping and Portscanning operations.

Please Note: Operations are available only when Firewall is enabled from the **Firewall and NAT** page.

The page offers the following components:

The **Ping Stealth** checkbox selection prohibits a Ping operation toward Quadro from its WAN.

The **Fool Portscanner** checkbox selection prohibits Quadro portscanning from its WAN. As a reply to a Portscanning operation, "network unreachable" or "host unreachable" feedback messages will be sent.
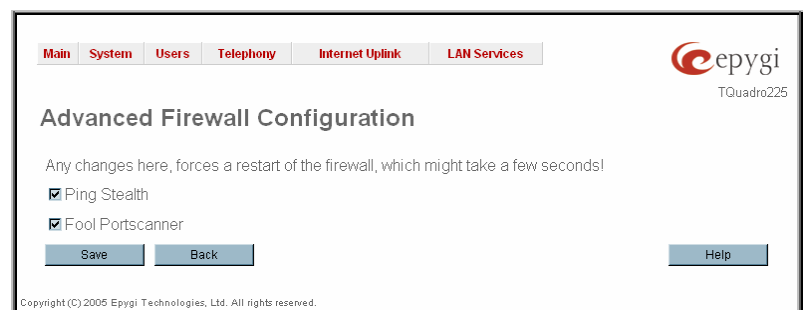
Fig. II-142: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows the configuration of filters for the incoming and outgoing traffic.

To prevent misconfiguration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. As the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled (additionally NAT should be enabled to

use the **Port Forwarding** function in the **Incoming Traffic / Port Forwarding** filtering rules). The filtering rules are independent from the security level, so they will work if enabled, no matter what security level has been selected.

Please Note: Applying firewall rules will just prevent the establishment of new connections that violate the rules. Applying rules does not kill existing connections that violate the rule.

View All displays all configured filters specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). As it is read-only, no modifications are allowed and no functional buttons are available.

The **Incoming Traffic/Port Forwarding** filter is for incoming traffic. The rules here allow or deny systems on the Internet to reach the services of Quadro's LAN. NAT service should be enabled on the Quadro to provide the possibility of **Port Forwarding** in the **Incoming Traffic/Port Forwarding** filtering rules. The **Port Forwarding** function will be unavailable if NAT is disabled on the Quadro.

The **Outgoing Traffic** filter is for outgoing traffic. The rules here allow or deny Quadro's LAN users to reach external services.

Management Access is used to enable management access to the Quadro from the Internet. A host on the Internet can be allowed to reach the Quadro.

SIP Access is to allow or deny the SIP access to or from the particular SIP servers, SIP hosts or a group of them. The **SIP Access** filtering rule may prevent or allow incoming or outgoing SIP calls to or from specified SIP server(s) or host(s).

When **Blocked IP List** is used, traffic from specific hosts may be blocked, no matter what services are opened in the other filters. NO traffic will be allowed to the specified hosts. The **Blocked IP List** service has a higher priority if the same host is also listed in the **Allowed IP List** table.

Allowed IP List allows trusted hosts to reach your network and vice versa. It is an exception to other rules and only all services may be allowed for a single host.

Restricted IPSec - Generally hosts in a VPN are allowed to have access to any service, i.e., no traffic will be blocked. They are treated as if they were part of the Quadro LAN. However, this service can be manually denied here.

Fig. II-143: Filtering Rules page

The **Filtering Rules** page provides several links. Each link opens its specific parameters on the same page. Only **Change Policy** (see chapter Firewall and NAT), **Manage user Defined Services** (see chapter Service Pool) and **Manage IP Pool Groups** (see chapter IP Pool) are leading to separate pages. The **Filtering Rules** page also includes the currently selected firewall security (**Policy**) level and its description.

The table displayed on the bottom of the page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the "No record(s) selected" error occurs.

- **Disable** is used to disable the rule. If no records are selected the "No record(s) selected" error occurs.

- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action,** a **Restriction** to certain IP address(es) or IP groups, and if adding a rule for **Incoming Traffic/Port Forwarding**, the destination IP address for **Forwarding:**

For example, the page to add a rule for **Incoming Traffic/Port Forwarding** offers the following input options:

Service includes a list of possible services to be configured. All user defined services also will be displayed in this list.

Action includes possible actions to setup the rule.

Forward to IP requires the destination IP address where traffic should be transferred to, if it comes from the restricted host. The IP address defined in this field will be ignored for blocked action of the **Incoming Traffic/Port Forwarding** rule.

Note: It is not allowed to forward incoming packets when NAT service is disabled on the Quadro.

Port Translation text field is available for "Allowed" action only and optionally requires the port number that will stand instead of original port number when incoming packet is being forwarded. If this field is left empty, original port number will be used upon forwarding the packet.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.

- Selecting **Single IP** will require the IP address of the allowed or blocked host.

- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. **Maskbit** examples:
  255.0.0.0= /8,
  255.255.0.0 = /16,
  255.255.255.0 = /24,
  255.255.255.255= /32

- **Group** indicates the user defined groups that include IP addresses that ought to be allowed or blocked.

Description field is used to insert an optional description of the filtering rule.

Fig. II-144: Filtering Rules - Page to add a rule for Incoming Traffic

---

To Add a Filtering Rule

1. Select the **Filter** link (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List, Allowed IP List or Restricting IPSec) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the **Filtering Rules** page. A page where a new rule may be added will appear in the browser window. The page will be named corresponding to the selected filter.
3. Select a service name from the **Service** list to configure a rule for it. If the list has a default value, leave it as is.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, leave it as is.
5. Enter the IP address in the **Forward to IP** field if an **Incoming Traffic Rule** is to be added.
6. Choose the restriction type by selecting **Any**, **SingleIP** or **IP/Mask** and enter the required information in the text fields or select a group.
7. Insert a **Description**, if needed.
8. To add a rule with these parameters press **Save**.

To Delete Filtering Rules

1. Select the **Filter** link to delete a rule from its table. The appropriate **Filter** table will appear in the same window.
2. Check one or more checkboxes of the corresponding rules that ought to be deleted from the rules table. Press **Select all** if all rules ought to be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion with **Yes**, or cancel it with **No**.

Service Pool

The **Service Pool** table is a list of all created services and their parameters. It is used to add new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or permission by defining a new filtering rule:

Add opens the **Add New Service** page where new services may be added.

Edit opens the **Edit Service** page where the service parameters (except for the service name) can be modified. This page includes the same components as the **Add New Service** page. To operate with **Edit** only one record may be selected, otherwise an error will occur: "One row must be selected".

Fig. II-145: Service Pool page

The **Add** page is used to add new services and includes the following text fields and buttons:

Service Name requires a name for the service that ought to be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.
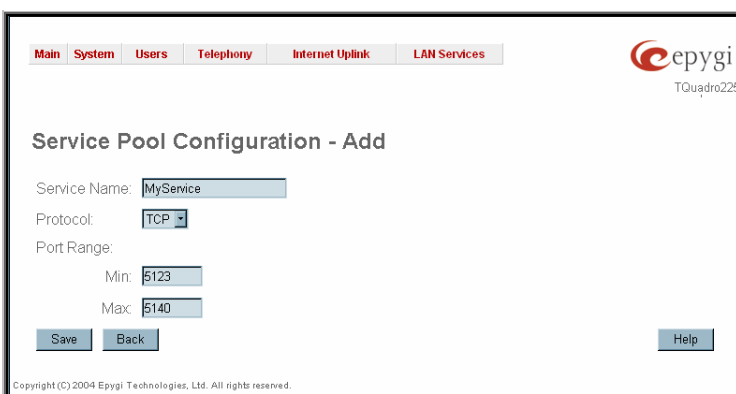
Fig. II-146: Service Pool - Page to add a new Service

To Add a new Service

1. Select the **Manage User Defined Services** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **Service Pool Configuration** page. A page where a new service may be added will appear in the browser window.
3. Define a service name in the **Service Name** text field.
4. Select the protocol type for the service from the **Protocol** drop down list.
5. Enter the port range in the **Port Range** text fields or leave one of them empty to define a particular port for the service.
6. To add a service with these parameters click on **Save**.

To Delete a Service

1. Select the **Manage User Defined Services** link. The **Service Pool Configuration** page appears with the table of services (if any).
2. Check one or more checkboxes of the corresponding services that ought to be deleted from the **Service Pool** table. Press **Select all** if all services ought to be deleted.
3. Click on the **Delete** button on the **Service Pool Configuration** page.
4. Confirm the deletion with **Yes**, or cancel it with **No**.

IP Pool

The **Manage IP Pool Groups** link opens the **IP Pool Configuration** page.

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. Whenever adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.

Fig. II-147: IP Pool Configuration page

Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise an error will occur: "One row must be selected".

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains).

Clicking on the **Group** name will display an **IP Pool Group Configuration** page with the **Members** list for the current group.

Fig. II-148: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise an error will occur: "One row must be selected".

Fig. II-149: IP Pool Group Configuration page

The **Add Members** page provides the following radio buttons:

IPaddress requires the member IP address that is to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

The **User-defined Group** includes previously added groups that also may be added as a member to another group.

Member description text fields can be used to enter an optional description of the member.

Fig. II-150: IP Pool Group Configuration – Add Member

To Add a new Group with Members
1. Select the **Manage IP Pool Groups** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **IP Pool Configuration** page. A page where a new group may be added will appear in the browser window.
3. Define a group name in the **Group Name** text field and fill in the **Group Description**, if needed.
4. To add a group with the given parameters press **Save**.
5. Open the **IP Pool Group Configuration** page by clicking on the group name.
6. Select the **Add** button on the **IP Pool Group Configuration** page. A page opens where new members may be added to the group.
7. Enter an IP address for the member in the **IP Address** text fields, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
8. Enter a **Member Description** in the corresponding text field, if needed.
9. To add a member with these parameters to the selected group press **Save**.

To Delete a Member
1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Click on the desired members that ought to be deleted. The **IP Pool Group Configuration** list appears.
3. Check one or more checkboxes of the corresponding members that ought to be deleted from the **Members** table. Press **Select all** if all members ought to be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.

5. Confirm the deletion with **Yes** or quit with **No**.

To Delete a Group

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Check the one or more checkboxes of the corresponding groups that ought to be deleted from the groups table. Press **Select all** if all groups ought to be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion with **Yes** or quit with **No**.

LAN Services Menu

Fig. II-151: LAN Services menu in Dynamo theme

Fig. II-152: LAN Services menu in Plain theme

DNS Settings

The **DNS Settings** page gives the possibility to setup a name server for the Quadro. It offers the following components:

Nameserver Assignment radio buttons:

- **Dynamically by provider** selection automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** is a manually selected name server. The **Nameserver** text field requires the IP address of an external name server. The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.
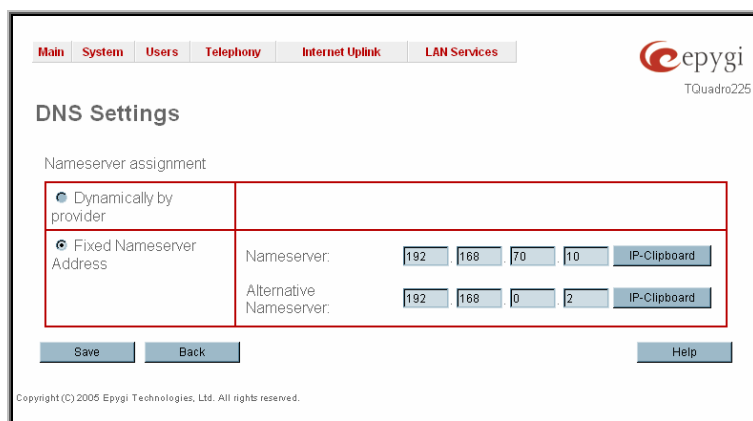
Fig. II-153: DNS Settings page

DHCP Settings for the LAN Interface

The **DHCP Settings** page gives the possibility to enable a DHCP server and control the Quadro user's LAN settings. Thus Quadro LAN users will be provided automatically with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the Quadro's IP address)
- WINS server
- Nameserver (corresponds to the Quadro's IP address)
- Domain name

The **DHCP Settings** page offers the following input options:

Enable DHCP Server activates the DHCP server on Quadro.

IP Address Range defines a range of IP addresses that will be assigned to the Quadro LAN users. The IP range must be at least six, otherwise the "Address Range too small" error will prevent saving. The "Address Range too large" error occurs if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the Quadro LAN users.

View DHCP Leases leads to the page where the DHCP leased LAN IP addresses are listed.
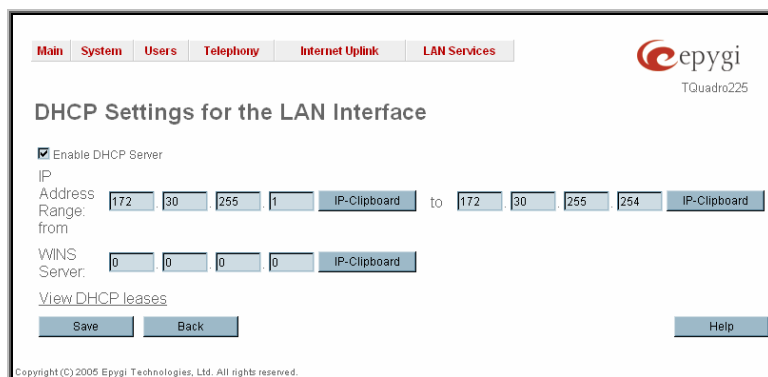
Fig. II-154: DHCP Settings page for LAN interface

The **DHCP Leased IP Addresses** page includes a list of the leased host addresses that are part of the Quadro's LAN. For these hosts, Quadro acts as a server supplying them with a unique IP address. It displays a read-only table describing all the leased IP hosts and their parameters. The table contains the following columns:

IP address - host IP address, assigned by Quadro.

MAC address - host MAC address, provided by the host itself.

Lease Start - date and time when the leased IP address has been activated.

Lease End - date and time when the leased IP address has been or will be deactivated.

Hostname - hostname, provided by the host itself.

Fig. II-155: DHCP Leases page for LAN interface

Registration Form

The **Registration Form** page appears when administrating an unregistered Quadro, and has been established for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It provides several links offering registration options:

Register now leads to the Epygi Technical Support System Registration page and requires customer's information to submit the Quadro registration form.

Remind me later hides the registration notification until the next administrating the Quadro through System Configuration Wizard or Internet Configuration Wizard.

Don't remind me more hides the registration notification forever.

Fig. II-156: Device Registration page

Administrator's Additional Features

Incoming Call Blocking and Outgoing Call Blocking

The **Incoming Call Blocking** and **Outgoing Call Blocking** pages offer extended features for the administrator to activate incoming/outgoing call blocking services for certain callers. This configuration cannot be changed by the users.

For more information on the **Call Blocking Settings** pages, see Incoming Call Blocking and Outgoing Call Blocking chapters of the Extensions Users Guide - Manual III.

The **Call Blocking** pages accessed from **Caller ID Based Services** table by clicking on the corresponding address, give administrator a possibility to enable blocking services which could not be disabled by the users.

Besides the components seen for the user, an additional **Protect this entry** checkbox is available in the **Call Blocking - Add Entry** pages for administrator access only. With this checkbox selected, user will be unable to deactivate the blocking services configured by administrator.

Fig. II-157: Blocking Page for the Administrator

Logout

This option is used to close the session between the user PC and Quadro and to leave the Quadro Web Management or to enter the management with another login. By selecting the **Logout** button, the startup page will be displayed and the user needs to login again.

Administrator Login

At the moment, the administrator login allows only the modification of the auto attendant (AA) greeting and Universal Extension Messages. After dialing ✱❼❺, use key ❶ to enter the auto attendant greeting menu, ❷ to enter auto attendant menu messages menu and use key ❸ to enter the Universal Extension Messages menu. The key combinations beside are available to modify the auto attendant greetings.

✱❼❺ **Administrator's Login**						
❶ Auto Attendant Greeting	❷ Auto Attendant Menu Message	❸ Universal Extension Messages				
❶ Listen to Current AA Greeting	❶ Listen to AA Menu Message	❶ Greeting Message	❷ End of Greeting Message	❸ Incoming Blocking Message	❹ Outgoing Blocking Message	❻ Out of Office Message
❷ Record a New AA Greeting	❷ Record a New AA Menu Message	❶ Listen to Current Greeting Message	❶ Listen to Current End of Greeting Message	❶ Listen to Current Incoming Blocking Message	❶ Listen to Current Outgoing Blocking Message	❶ Listen to Current Out of Office Message
❸ Restore Default AA Greeting	❸ Restore Default AA Menu Message	❷ Record a Universal Greeting Message	❷ Record a Universal End of Greeting Message	❷ Record a Universal Incoming Blocking Message	❷ Record a Universal Outgoing Blocking Message	❷ Record a Universal Out of Office Message
		❸ Restore System Default Greeting Message	❸ Restore System Default End of Greeting Message	❸ Restore System Default Incoming Blocking Message	❸ Restore System Default Outgoing Blocking Message	❸ Restore System Default Out of Office Message
# Stop Recording or Playback	# Stop Recording or Playback	# Stop Recording or Playback Greeting Message	# Stop Recording or Playback End of Greeting Message	# Stop Recording or Playback Incoming Blocking Message	# Stop Recording or Playback Outgoing Blocking Message	# Stop Recording or Playback Out of Office Message
✱⓿ Administrator's Logout						

Appendix: Extension Users Welcome Page

This welcome page may be helpful, if administrators want to inform their extension users about individual data, they need to use the extensions. Such as phone numbers, phone lines, IP addresses and SIP numbers. To get a word form that may be edited and sent by mail, double-click the paper clip on the right.

You are using a **Quadro IP PBX** made by Epygi Technologies, Ltd. This product incorporates SIPVoice™ Digital Signal Processing technology to send crystal clear voice around the globe without associated fees for long distance. But, you will soon learn, it does much more. Your **Quadro IP PBX, The Global Phone Network in a Box**, operates in much the same way as systems with which you are already familiar: a telephone, a PBX, voice mail, a phone book, et cetera. Beyond that the **Quadro IP PBX** provides capabilities you never believed were accessible in a customer premise telephony product. Soon you will experience the freedom and power of the **Quadro IP PBX, The Global Phone Network in a Box.**

To get started the following information is helpful.

PHONES

Your extension number is **<extension number>** and your password is **<password>** (optional).

Remember to type the **Auto Attendant number** when you pick up your phone receiver to find the WELCOME spot. ***0** will take you directly to voice mail for your extension. ***74** will confirm your extension number.

LOCAL PHONE LINES

Quadro2x and Quadro2xi offer one external phone line: **<1. local phone line>**

IP

To reach your Quadro IP PBX from a network connection inside your office, home or place of utilization, connect a Web browser to **<IP address>** (172.30.0.1 is the default IP address).

The email address of your Quadro IP PBX System Administrator is **<email address>**

His phone numbers are **<phone numbers>**

SIP

Your SIP number (an Internet phone number) is **<SIP number>**@sip.epygi.com.

This is a number you can give people to reach you.

The SIP number to reach the Auto Attendant of your local Quadro is **<SIP number>**@sip.epygi.com.

Your SIP group link to provide you a phone directory of numbers to call is:

http://www.epygi.com/sip/grp_view.php?viewgrp=**<groupname>**

The email address of your SIP System Administrator is **<email address>**

His phone numbers are **<phone numbers>**

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name -admin Password - 19
Quadro Hostname	quadro
LAN IP Address	172.30.0.1 Subnet Mask - 255.255.0.0
DHCP Server	Enabled, IP Range - 172.30.0.100-172.30.0.254, WINS - 0.0.0.0.
Regional Settings and Preferences	Locale – US, TimerZone - US/Central, Theme – Dynamo.
Emergency and PSTN codes	Emergency code -911, PSTN code – 9.
WAN Interface Protocol	Ethernet
WAN Interface Bandwidth	Upstream – 10000, Downstream – 10000, Min Data Rate – 0.
WAN IP	Automatically through DHCP
Mac Address	Assigned by device, MTU - 1500 Bytes.
DNS Server	Dynamically
IP Routing Configuration	No Routes
Event Settings	"Display notification" for all except Login event, which has "Do nothing" action assigned.
Time/Date Settings	NTP Server and Client – enabled, Predefined NTP Server - npi1.epygi.com, Polling interval – 6.
Mail Settings	Disabled
SMS Settings	Disabled
Features	IP Phone support - disabled
Language Pack	Default - English Custom Language Pack - none
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Extension (all accessible pages for extension), Local Administrators (all accessible pages for localadmin).
Extensions Management	00, 11-12, 31-32 extensions exist
Extension Settings – General	Display name – none, Password – empty, 11-12 extensions attached to the FXS lines 1-2, 31-32 extensions attached to the IP lines 1-2, Call Relay – disabled, Call Park – disabled, External Call Policy – disabled, Percentage of System Memory – 20%.
Extension Settings – SIP	Registration username and password - automatically generated, SIP server - sip.epygi.com, SIP Server port – 5060, SIP Server Registration – enabled.
Extension Settings – SIP Advanced	User ID – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP

Parameter	System Default Value
	Server – undefined.
Extension Settings – Remote	Remote Extension – disabled
Extension Settings – Call Queue	Call Queue – disabled
Extension Settings – Voice Mailbox	Extension 11 – Internal Voice Mail, Extension 12 – Disabled Voice Mail.
Extension Settings – Codecs	Codecs - G711u (preferred), G711a, G729a, G726/32, G726/16, G726/24, G726/40 Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Attendant 00 Settings – General	Display name – Attendant, FAX forwarding – disabled, Percentage of System Memory – 3%.
Attendant 00 Settings – Attendant Scenario	Scenario – default, Send AA digits to Routing Table – disabled, Welcome and Menu messages – default, Authorized Phones Database – undefined.
Attendant 00 Settings – SIP and SIP Advanced	Same as for an extension.
Attendant 00 Settings - Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, G723, iLBC Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Receptionist Management	No entries
Call Statistics	Enabled 100 entries for all type of calls
SIP Settings	UDP and TCP Port – 5060, Session Timer – disabled, DNS Server for SIP – default, SIP timers – RFC 3261.

RTP Settings	Properties for all Codecs except G723 and iLBC :
	    Packetization -20ms
	    Silence Suppression -yes
	G723 and iLBC properties:
	    Packetization - 30ms
	    Silence Suppression – yes
	RTP/RTCP port range for FXS lines - 6000-6049
	RTP/RTCP port range for IP lines - 6050-6099
	G276 Standard - ITU-T specification
	Telephone Event Draft Support - enabled
	RTCP Support - disabled

NAT Traversal Settings	NAT Traversal for SIP – force
	SIP and RTP Parameters - Use STUN
	SIP TCP Port – 5060
	STUN Parameters:
	    Primary STUN Server - stun.epygi.com
	    Primary STUN Port – 3478
	    Secondary STUN Server – undefined
	    Secondary STUN Port - undefined
	    Polling Interval: 1 hour
	    Keep-alive interval: 120 seconds
	    NAT IP checking interval: 300 seconds
	    No entries in NAT Exclusion table

Line Settings	Onboard Lines Configuration:
	    CallerID- Standard 2 FSK for all lines
	    Ringer type: Type A for all lines
	    Busy Tone and Power Disconnect indications: disabled for all lines

Parameter	System Default Value
	Off-hook caller ID - disabled for all lines IP Lines Configuration: 　1-2 IP Lines exist. IP Lines 1 and 2 are enabled and attached to 31 and 32 extensions. 　FXS Lines Loopback Settings – Loopback is disabled for all FXS lines, Loopback timeout is 30.
FXO Settings	FXO line – enabled, incoming and outgoing calls allowed and routed to 00 Attendant on both, Use FXO lines of the other device – disabled.
ISDN Settings	ISDN Trunks - Trunk 0 and Trunk 1. Settings for both Trunks: 　State – started, 　Interface – User, 　Coding Type - a-law, 　Loopback mode - no loopback, 　Passive Mode – disabled, Signaling settings for both Trunks: 　DID Service – disabled, 　TEI Mode – Automat, TEI Assignment on Power up – enabled, 　MSN Settings - No other devices connected to ISDN bus, 　Route Incoming Call to - 00, 　Use Default outgoing MSN – enabled, 　Default outgoing MSN – none, 　Excessive Ack. delay T200 – 4000, 　Idle timer T203 – 10000, 　T302 timer – 4000 　T309 timer – 0, 　T310 timer – 60000, 　After Guard Timeout -150, 　Switch type - basic_dss1, 　Channel Selection – preferred, 　Bearer Establishment Procedure - on call acceptance, 　Called Party Type of Number – unknown, 　Calling Party Type of Number – unknown, 　Called Party Numbering Plan – ISDN/telephony numbering plan, 　Calling Party Numbering Plan – ISDN/telephony numbering plan, 　Incoming Called Digits Size – 0, 　Generate Progress Tone to IP – disabled, 　Enable CLIR Service – disabled, 　Alternative Disconnection Mode – enabled, 　B1 and B2 channels – enabled.
Gain Control Settings	FXS lines: Transmit Gain: - 6 Receive Gain: 0 FXO lines: Transmit Gain: 0 Receive Gain: 6 ISDN Trunks: Transmit Gain: 0 Receive Gain: 0
Call Routing	Route all incoming SIP calls to Call Routing - disabled Local Routing table - 6 entries for FXO Quadros and 4 entries for ISDN Quadros. Entries are defined for IP, PBX and PSTN calls establishment. Local AAA Table - no entries.
RADIUS Settings	RADIUS client - disabled
Voice Mail Common Settings	Voice Mail Recording - G729a Memory Allocation - Embedded Memory Storage
Dial Timeouts	4 seconds
IPSec, PPTP and L2TP	No connections
Dynamic DNS	Disabled
Firewall	Enabled, Medium level, Ping Stealth - enabled Fool Portscanner - disabled
NAT	Enabled
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all), SIP Access (Allowed for all),

Parameter	System Default Value
	No user defined services and IP pool groups

Extension Settings

Parameter	System Default Value
Voice Mail Settings	Maximal mail message duration - 5 min, Send end of greeting message – disabled, Ask password before granting local access to mail box – disabled, Ask password before granting remote access to mail box – enabled, Send welcome message – disabled, Play Voice Mail help – enabled, Automatically play messages - enabled, Send mails count information message – disabled, Send date/time information message – enabled, Send beep at the end of message – enabled, Send new voice messages via e-mail – disabled, Send new voice message notifications via SMS – disabled, Send new voice message notifications via phone call – disabled, Voice Mail Indication - Tone indication, Zero Out – enabled, to 00 default Attendant, FAX Redirection – disabled, Out of Office – disabled, Greeting message – default.
Group List	No entries
Speed Calling	No entries
Account Settings	Display Name – undefined, User Password Protection – disabled both for incoming and outgoing calls, Custom Voice Messages – default.
Caller ID Based Services	No entries in the table. For Any Callers – all services disabled, Blocking Voice Messages – default.
Basic Services - General	No answer timeout – 20 sec, Call Waiting Service – enabled, Autoredial Interval - 10 sec, Autoredial Period - 15 min.
Basic Services - Hold Music	Send Hold Music to remote party – disabled, Hold Music - Own Music. Music file – default
Basic Services - Do Not Disturb	Disabled. Timeout - 30 min, Send message to Caller Party – enabled.
Basic Services - Hotline	Disabled

Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD.
Software License Agreement

> **THIS IS A CONTRACT**.
> CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE HARDWARE OR SOFTWARE.

1.   **License.** Epygi Technologies, Ltd. (the "Licensor"), hereby grants to you a non-exclusive right to use the Quadro Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may use the Licensed Materials only in connection with your operation of your Quadro. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.

2.   **Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or the transfer of the Licensed Materials is subject to the terms of this Agreement.

3.   **Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.

4.   **No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language under penalty of law.

5.   **Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro-2x or any Quadro SIP Gateway product. If you sell your license rights in the Licensed Materials you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

6.   **Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.

7.   **Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES AND ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

8.   **LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OF OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.

The foregoing limitation, exclusion and disclaimers apply to the maximum extent permitted by applicable law.

9.   **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

10.   **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227-19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.

11.   **Entire Agreement.** It is understood that this Agreement, along with the Quadro Installation Guide and User's Manual, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.

12.   **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.

13.   **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.

14.   **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.

If you have any questions about this Agreement, please write to Epygi at 6900 North Dallas Parkway, Suite 850, Plano, Texas 75024 or call Epygi at (972) 692-1166.